2007-02

# Homeland Security Affairs Journal, Volume III - 2007: Issue 1, February

Monterey, California. Naval Postgraduate School

Homeland Security Affairs Journal, Volume III - 2007: Issue 1, February
https://hdl.handle.net/10945/49814

VOLUME III, ISSUE 1: FEBRUARY 2007

# HOMELAND SECURITY AFFAIRS

THE JOURNAL OF THE
NAVAL POSTGRADUATE SCHOOL CENTER FOR HOMELAND DEFENSE AND SECURITY





ISSN 1558-643X HTTP://WWW.HSAJ.ORG

# Changing Homeland Security: Ten Essential Homeland Security Books

Christopher Bellavita

This article presents what I consider to be ten essential homeland security books. The list is personal and provisional. The discipline is too new to have a canon. We need to continuously examine what is signal and what is background noise in homeland security's academic environment.

Much has been written about homeland security. A lot more is in the publishing pipeline. My list includes books I find myself returning to as I seek to understand contemporary homeland security events. Beyond personal interest, I believe they form a foundation for a growing understanding of the parameters of what it means to study homeland security as a professional discipline. Other books – and important articles – could be added, but ten is sufficient to start.

These books are:

- *The Final Report of the National Commission on Terrorist Attacks Upon the United States: 9/11 Commission Report* (2004)
- *The National Strategy for Homeland Security* (2002)
- *After: How America Confronted the September 12 Era* (2003)
- *Imperial Hubris: Why the West is Losing the War on Terror* (2004)
- *America the Vulnerable: How Our Government is Failing to Protect Us From Terrorism* (2004)
- *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism* (2005)
- *Catastrophe Preparation and Prevention for Law Enforcement Professionals* (2008)
- *Trapped in the War on Terror* (2006)
- *Unconquerable Nation: Knowing Our Enemy; Strengthening Ourselves* (2006)
- *The Declaration of Independence* (1776), *The Articles of Confederation* (1777), and *The Constitution of the United States of America* (1787)

Taken together, these works outline a broad historical narrative about homeland security. We were attacked. We quickly developed a strategy to make sure we prevented future attacks. We tried to come to terms with what happened to us as a nation. Next, textbooks and workbooks aiming to systematize homeland security ideas started to appear. Homeland security took the first steps toward becoming institutionalized. Then came the criticism of how we perceived the enemy and what we were doing – or not

doing – to protect the homeland. Recently, some people maintain we have significantly overreacted to the threat and are now "trapped" in a War on Terror that accomplishes little, wastes resources and threatens our national values. Others urge government to focus resources on threats that have the potential to cause us the greatest damage and to encourage communities to become resilient. The American people must be willing to accept some level of risk. While there is a threat of attack by terrorists, there is a bigger danger that how we react will do more damage than the attack. As one of the authors cited later in this essay wrote: "Instead of surrendering our liberties in the name of security, we must embrace liberty as the source and sustenance of our security." Homeland security gets better through the open exchange of competing and contrasting ideas. Keeping this essential debate open and free helps ensure we will remain an "Unconquerable Nation."

## *The Final Report of the National Commission on Terrorist Attacks Upon the United States: 9/11 Commission Report*[1]

Not many government reports are literary enough to be nominated for the National Book Award. The *9/11 Report* was.[2] The *Report* chronicles the events that led to a perceived need for something called homeland security. It provides an analysis of why we were attacked and why the attack succeeded. It outlines what the nation needs to do to reduce the chances that we will be unprepared for another attack. It provides continually relevant benchmarks against which to assess the status of efforts to protect the nation from terrorism.

The book begins with a prosaically clinical retelling of what happened on a day that "dawned temperate and nearly cloudless in the Eastern United States." [1] Chapter One ends with a quote from an unknown NORAD member who observes "This is a new type of war."

In an extended flashback, the authors use Chapters Two through Eight to discuss the foundations of this new type of war. They focus on the origins and rise of Osama bin Laden and al Qaeda. They detail how al Qaeda prepared for the attack. They present the reader with a portrait of the enemy as "sophisticated, patient, disciplined, and lethal." It is the chilling image that persists today. The nation continues to struggle to understand who the enemy is and what it wants.

The report describes how

> [T]he institutions charged with protecting our borders, civil aviation, and national security did not understand how grave this threat could be, and did not adjust their policies, plans and practices to deter or defeat it. We learned of fault lines within our government – between foreign and domestic intelligence, and between and within agencies. We learned of the pervasive problems of managing and sharing information across a large and unwieldy government that had been built in a different era to confront different dangers. [xvii]

According to the Report Card issued by the vestiges of the 911 Commission and to the "First 100 Days" agenda of the 110th Congress, many of those institutional problems persist.

The *9/11 Report* concludes the attack happened because of the failure of imagination, policy, capabilities, and management. It is interesting (although understandable from a political perspective) that the Commission chose to focus on the failure of "management" rather than "leadership." Usually when big things go wrong leaders, not managers, are responsible. The Commission avoided making a judgment about how and which leaders failed.

The *9/11 Report* tetrad creates a framework for assessing preparedness: Do we have the right policies? Do we have the capabilities to execute those policies? Do we have the appropriate leadership in homeland security? Do we encourage and use imagination where it can do the most good?

Homeland security efforts since the *Report* was published have focused primarily on improving response capabilities and on policy. Much less emphasis has been placed on what it means to be an effective homeland security leader, or on systematically developing those leaders. It is unclear how to – or whether we should – institutionalize imagination. There continues to be more basic homeland security work to do than anyone, including contractors, has time to do well. One can barely wonder what a more imaginative workload would look like. On the other hand, there is a growing view (discussed later in this essay) that perhaps we have become more imaginative about the terrorist threat than is warranted by the empirical evidence.

The 9/11 report was criticized almost the same day it was released.[3] But the report – along with the transcripts and audio and video recordings of the testimony that contributed to the Commission's findings – will remain a historically important artifact as long as homeland security remains a function of government. The *9/11 Report* is essential because it reminds us what life was like before and on that singular Tuesday in September.

## *The National Strategy for Homeland Security*[4]

*The National Strategy for Homeland Security* is one of the first comprehensive efforts to describe a domestic public policy strategy. Formal strategy documents are routine in the Department of Defense and national security world. They are less prevalent in the domestic policy arena.

There are extensive debates about what a strategy is.[5] I find it useful to consider strategy as both intentional and emergent.[6] *The National Strategy for Homeland Security* is intentional. We were attacked. We had to respond. What should we do? One approach would be simply to have individual agencies decide what to do, then coordinate that effort through the usual government mechanisms. Another way is to coordinate

those efforts within a unified design. That is what the *National Strategy* intends to do.

The *Strategy* is paved with good intentions. But in my experience it is rarely referred to outside a relatively small circle of people and agencies. When it was first released it was criticized as less of a strategy and more a huge to-do list. One critic said it had more activities than his daughter's summer camp. A primary author of the *Strategy* responded that while that was an amusing debate point, "what I haven't heard is anyone say that we missed anything and I haven't heard anyone say that any of the 84 [activities in the Strategy] don't matter."[7]

The *Strategy* is a "theory for how we're going to cause security for ourselves."[8] It aims to address four basic, and complex, questions: What is homeland security and what are its missions? What are we trying to accomplish and what are the most important goals? What is the national government doing now to achieve those goals and what should they be doing? What should state, local, tribal, private sector entities, and citizens do to help make the nation secure?

One definition of "strategy" says that it is the bridge between policy and operations.[9] Clearly, this document is not that kind of strategy. There is no one place to go to find *the* national homeland security policy. Instead, the nation's homeland security policy has to be constructed retrospectively by aggregating laws, presidential directives, grant guidance, and other regulatory documents. The *National Strategy* is better seen as a Grand Strategy. It is "a high level statement of what we're trying to do."[10]

One wonders what the relationship is between the strategy that is outlined in this document and the strategy that has emerged over the last few years. For example, the official definition of homeland security says "Homeland Security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." [2]. These are straight forward words. Homeland Security is about terrorism. The first strategic objective is to prevent terrorism. If it were not for terrorism, there would be no large-scale government activity called Homeland Security. There is nothing in the definition, and precious little in the strategy (maybe 5 percent), about all hazards, natural disasters, or pandemics.

One should not be so doctrinaire to think that a written strategy is or should be the primary driver of government's behavior. The world did not stop after 9/11. Katrina demonstrated gaps in our response capabilities. Avian flu raised the specter of the 1918 pandemic and called attention to the inadequacies of our public health and medical care system. The real homeland security strategy that emerges in parallel with the written *National Strategy* seems to change priorities according to whatever the last disaster was or the next credible catastrophe might be. That is a reminder that what government does is shaped more by politics than paper.

The official *Strategy* does a number of structural things well. It describes – at the 50,000 foot level – the threats and where we are vulnerable to those threats. It outlines how the nation is organized to meet those threats, reminding readers of the role of federalism. It identifies six mission areas which, in July 2002, seemed especially critical: intelligence, border and transportation security, domestic counterterrorism, critical infrastructure, catastrophic threats, and emergency response. Five years later these issues still represent sources of national distress.

The strategy describes what it terms four foundations that cut across all the mission areas: law, science and technology, information sharing, and international cooperation. It believes these foundations can be used as the basis for deciding where to invest resources. One could argue whether these are foundations, other mission areas, or the framework for the homeland security industrial complex. But they add to the effort to provide a comprehensive conceptual look at what it will take to prevent and respond to the next attack.

A useful strategy describes ends, ways, and means. *The National Strategy* does pay some attention to the costs of homeland security. It notes we spend (as of 2002) roughly $100 billion a year on homeland security. It asserts that "as a Nation we will spend whatever is necessary to secure the homeland." [63] There is no evidence given to support the $100 billion a year figure. Unless I missed it somewhere, there is no authoritative accounting anywhere of just how much homeland security costs the nation. There is little incentive to know. There is no mechanism – except perhaps Congress – for discovering. There is no agreed upon set of categories to establish what even counts as homeland security spending.

The *National Strategy for Homeland Security* is showing its age. There is a glaring gap between the strategy's emphasis on prevention and the financial and political support for response. According to the *Strategy*, homeland security is supposed to be almost exclusively about terrorism. Congressional hearings, budgets, assessments, and documents suggest homeland security increasingly is about all hazards.

The *National Strategy* anticipates that it will be "adjusted and amended" over time. It is now appropriate that the nation develop a new strategy, based on the lessons we ought to have learned over the past five years. This should be one of the first items of business for a new congress and a new administration. But there is nothing that says a national strategy has to come from the central government. The National Governors Association, the National Homeland Security Consortium, National League of Cities, among others, are just as capable of initiating overall direction for the nation, especially in a networked world.

While some of what is in the current *Strategy* should be changed, other elements should be carried over to version 2.0 – if not in specifics, at least in philosophy. For example, there are eight principles that guided the design of the first *National Strategy*:

- Require responsibility and accountability,
- Mobilize the entire nation,
- Manage risks and allocate resources judiciously,
- Seek opportunities out of the adversity created by having to pay attention to terrorism,
- Foster flexibility in the nation's homeland security programs,
- Measure preparedness,
- Sustain preparedness, and
- Constrain government spending.

These may not be the only or the best principles to inform a national strategy. But they are worth considering for future iterations.

For now, however, we work with the strategy we have. *The National Strategy for Homeland Security* is clear enough to say where we should be going, and flexible enough to encourage the nation to consider what it means to have an effective strategy.

### *After: How American Confronted the September 12 Era*, by Steven Brill[11]

Here is the narrative so far: the nation was cruising along as the world's only super power. There were distant threats, but for the most part we were on top of history. All that was left was for everyone to get rich. Then we were attacked by an enemy who had been at war with us for at least twenty years. This time they got our full attention. We developed a strategy for dealing with the enemy, and in the process began to reshape the nature of our government, its relationship to the world, and its relationship to its people.

Steven Brill captures what happened during the period from September 12, 2001 to January 2003. In a brief prologue he introduces the main characters in his story and what they were doing on September 11th. Part One, called "Climbing Back," covers the period from September 12 through October 12, the first frightening and numbing month after the attack. Part Two, "New Routines, New Systems" describes October 15, 2001 to December 31, 2001. Part Three covers January 2 through June 10, 2002, a period of "Short Term Pain and Gain, Long Term Plans." Part Four, "Coming to Terms With The New Era" describes the period of June 12 through September 11, 2002. The Epilogue closes the narrative in January 2003.

The story unfolds through the experiences of people. A customs inspector has to deal with how to make sure there is no nuclear bomb in his port. A California businessman who produces luggage screening devices sees the event as both a tragedy and as a business opportunity.

There is a sharp contrast between Attorney General Ashcroft – who wants to make sure nothing like this happens again and who authorizes the questioning and detaining of hundreds and maybe thousands of people – and the recently hired executive director of the American Civil Liberties Union, who tries to hold back efforts he perceives will corrode civil liberties. The chief executive of a major insurance company has to decide whether his company will pay or avoid insurance damages. The Red Cross director has to figure out how to collect and distribute unprecedented donations, and at the same time avoid attacks by her board of directors. A small business man – the owner of a shoe repair business – has to rebuild his business. A border patrol agent speaks publicly about his section of unprotected border and faces practically unending efforts by the bureaucracy to fire him.

While all this is going on, Tom Ridge and a very small group of people develop first an Office of Homeland Security and then a Department of Homeland Security. There are many remarkable stories in this 700 page book. The best one – for those with an interest in homeland security politics – may be the story of how Ridge and his group encounter bureaucratic, political, and other barriers while trying to create a new way of doing business in the executive and congressional branches.

Pennsylvania Governor Tom Ridge was in a relative's hospital room when the planes attacked. A few days later he was selected to run the White House-based Office of Homeland Security and carry out a strategy that required coordinating other executive branch agencies. Brill describes the massive problems Ridge faced getting agencies to think beyond their organizational province. Ridge's relationship to those agencies changed after he was named to head the new Department of Homeland Security.

But from his first days in Washington, having to respond to the threat of the day – from anthrax attacks to problems with unsecured manhole covers – created an environment that gave Ridge and his staff little opportunity to think deliberately and comprehensively about what needed to be done. One early member of DHS described the pace as "having to fly a plane while you're still building it."[12] Brill illustrates how intention and happenstance combined to create that environment, one that continues to challenge the department.

This collection of stories is essential to understanding homeland security's early days – not just the Department of Homeland Security, but the complexity that faced the nation and its leaders after the attack. It is a truism that those who forget the past are condemned to repeat it. It has also been said that "those who remember the past are condemned to making the opposite mistake."[13] There is no way to operate with authority in the homeland security world without risking mistakes. Brill's book reminds the reader of the forces well-intentioned people encounter. Significant decisions have to be made in the absence of information; individual and organizational risks have to be taken. Politics, career issues, economics, networks, personal flaws, personal courage, and organizational

processes shaped what happened in the days after 9/11. The same dynamics continue to shape what we do today. I do not know a better book for describing those dynamics.

### *Imperial Hubris: Why The West Is Losing The War on Terror*, Michael Scheuer, writing as Anonymous.[14]

"If you know the enemy and know yourself," Sun Tzu advised centuries ago, "you need not fear the results of a hundred battles." Michael Scheuer argues we are losing the war on terror because we fundamentally misunderstand the enemy and what it wants. This is a war that "has the potential to last beyond our children's lifetimes and to be fought mostly on U.S. soil." [xi]

If you ask people who our enemy is you are likely to get the answer "terrorists." If you press, you will get the name al Qaeda. If you push further and ask what the enemy wants, you may get something like, "they hate us for our freedom and they want to destroy our civilization and our culture."

Michael Scheuer was one of the first people to argue that they – radical Muslim terrorists – do not hate us for our freedoms; they hate our policies. His writing calls attention to our lack of substantive knowledge about "the enemy" and what they want. As a former CIA analyst, Scheuer spent twenty-two years in the intelligence community, eight of those years studying al Qaeda. For Scheuer, the nation's initial homeland security strategy was based on faulty assumptions. In his view, we are fighting a worldwide battle against Muslim fundamentalists – not criminals or terrorists.

Bin Laden, as surrogate for the broader presumed clash of Muslim and Judeo-Christian civilizations, has been very clear about his foreign policy goals: the end to the Jewish state, the withdrawal of all U.S. and western military forces from the Arabian Peninsula, the end of all U.S. involvement in Iraq and Afghanistan, the end of U.S. support for governments that oppress Muslims, full Muslim control over the Islamic world's energy resources, and replacing U.S. backed Muslim regimes with governments that rule according to Islamic law. [210]

Scheuer writes that al Qaeda will attack the nation again; the next assault will involve weapons of mass destruction and be larger than the 9/11 attack. He wrote *Imperial Hubris* to show "there has never been a shortage of knowledge about the nature and immediacy of the...threat, but only a lack of courage to tell the truth about it fully, openly, and with disregard for the career-related consequences of truth telling." [xii]

I included this book in my list of essentials because it challenges orthodoxy. Specifically it challenges one-dimensional thinking about the enemy. More generally it demonstrates important tenants of critical thinking: identify core assumptions, subject the assumptions to data- and value-based analysis and evaluation, and offer conclusions that can be

further exposed to critical analysis. Significant parts of homeland security involve learning while one is doing. Effective learning requires not only critical thinking, but the personal and organizational courage to challenge conventional wisdom. *Imperial Hubris* demonstrates how that can be done.

Scheuer no longer works for the Central Intelligence Agency.

### *America The Vulnerable*, by Stephen Flynn[15]

"America remains dangerously unprepared to prevent and respond to a catastrophic terrorist attack on U.S. soil." [iv] Steven Flynn opens his 2004 book – *America The Vulnerable: How Our Government is Failing To Protect Us From Terrorism* – with those words. Michael Scheuer criticized the conventional understanding of the enemy. Flynn provides one of the first measured critiques of the nation's strategic, policy, and organizational response to September 11th. "If September 11, 2001, was a wake up call, clearly America has fallen back asleep," he writes.

Flynn was one of a small group who had a sense, before 9/11, of our nation's vulnerability to attacks. Flynn, like others who tried to get government to take the threat seriously, discovered that "Americans need a crisis to act. Nothing will change until we have a serious act of terrorism on U.S. soil." [xii] Flynn argues that after we were attacked, the nation reacted in a haphazard way, imposing poorly conceived security programs in an effort to do something – anything – to reassure the American public. His thesis in *America the Vulnerable* (amplified in his 2007 book *The Edge of Disaster*[16]) is that the nation remains unprepared for the next attack. In his view, the war on terror relies primarily on overseas military activities. The homeland has not been mobilized to confront the threat – whatever it might be. "Terrorism is a threat that we must constantly combat if we are to reduce it to manageable levels so that we can live lives free of fear." [xiii]

He outlines three "simplistic" positions offered in response to the attacks: security at any cost (whose advocates say we should pay any price to prevent terrorism on our soil); a Libertarian "cure is worse than the disease" school that does not want to impose any restrictions on the lives of individuals or the market (if we do, the terrorists have already won); or what he calls the "Go to the Source" approach – which he believes is the prevailing foundation for the war on terror. [10-11]

Flynn's primary caution is that al Qaeda has already demonstrated an ability to establish operations in the United States. They will do it again. Hence his emphasis on establishing a strong homeland security program. Flynn constructs a scenario of a simultaneous dirty bomb attack in New York, Michigan, New Jersey, Los Angeles, and Miami. He uses the scenario to "lament the fact that America has not spent its yesterdays preparing for the tomorrows that now confront the nation." [35] He believes we are in a "phony war," equivalent to the eight months after September 1939 when

the British and French declared war on Germany. Not much happened. Then the storm arrived. We wait for that storm today.

Flynn argues that as a people we do not yet have the maturity to live with the risks of future attacks and take reasonable precautions to manage risks. He devotes the middle part of his book to surveying the nation's most significant vulnerabilities – vulnerabilities which persist today. He notes that a government-only solution (i.e., DHS) fails to incorporate the involvement of citizens and the private sector. He then presents the audacious idea of replacing the current DHS-oriented national system with a Federal Security Reserve System, based on the political and organizational protocols of the Federal Reserve System (originally suggested by Ralph Lerner and extended by Flynn).[17] It is, to the best of my knowledge, the only significant alternative presented to the existing, not very carefully thought through, structure of the current homeland security system.

In our incremental society, the idea has practically no chance of becoming practice. DHS is going through its third reorganization in four years. There is little stomach for eliminating the department. But if we are attacked again; if the DHS system is found wanting; and if a new president, a new congress, and angry citizens say "Get us something different!" – then, perhaps, change will occur. For now, Flynn has few takers for the Federal Security Reserve System. It remains in the wings as a first class – and rare – example of a "big" homeland security idea.

Flynn takes a stab at answering probably the most difficult question in homeland security: how much security is enough? "We have done enough when the American people can conclude that a future attack on U.S. soil will be an exceptional event that does not require wholesale changes to how we go about our lives. This means they should be confident that the measures in place are sufficient to confront the danger." [164] He closes the book describing seven principles he believes will help us arrive at that end.

- There is no such thing as fail-safe security, and any attempt to achieve it will be counter productive.
- Security must always be a work in progress.
- Homeland Security requires forging and sustaining new partnerships at home and abroad.
- Our federalist system of government is a major asset.
- Emergency preparedness can save lives and significantly reduce the consequences of terrorist attacks.
- Homeland Security activities have deterrence value.
- Homeland Security activities will have derivative benefits for other public and private goods. [165-168]

Flynn's book is a mixture of evidence, interpretation, analysis, and opinion. He acknowledges that the book does not benefit from the kind of cautious study that characterizes traditional scholarship. It takes time and resources to do quality research. The homeland security research agenda is just getting started. Flynn acknowledges homeland security will benefit from the scholarly perspective that the passage of time will provide. But he believes time is not on our side.

Flynn models the role reflective practitioners can play in the development of homeland security's intellectual topography. His work is a harbinger that some of the best research in this emerging field will be done by the people who do homeland security work and who are grounded in the requirements of academic argument – whether positivists, constructionists, subjectivists, or of other methodological predispositions. All that is asked is that they present their ideas in a clear fashion, identify their assumptions and conclusions, and provide evidence that, if not convincing, is at least suggestive and supportive of the conclusions they reach. *American the Vulnerable* meets that test.

### ***Homeland Security: A Complete Guide to Understanding, Preventing and Surviving Terrorism,*** **by Mark Sauter and James Carafano**

One builds a professional discipline by developing a body of knowledge that evolves through research, practice and instruction. It is an open question whether homeland security will become a unique professional discipline, a specialization area for other professions, or turn into something presently unknown. The appearance of textbooks is one sign that a profession may be emerging. Mark Sauter and James Carafano are the authors of what I consider to be the best of a small batch of homeland security textbooks: *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism*.[18]

The almost 500 page book is not a "complete" guide. No work can be complete in this evolving enterprise. The book was written before Katrina, before the rise of pandemic flu concerns, and before the Second Stage (and now third stage) organizational changes. So there are dated parts of the text, such as: "The Department has four major directorates: Border and Transportation Security, Emergency Preparedness and Response; Science and Technology; and Information Analysis and Infrastructure Protection." [217] Such problems are inevitable.

The book is intended to be "a text for both academic and training courses in homeland security and terrorism." My sense is the book will be more useful for training programs and introductory undergraduate courses than for a graduate school audience. But anyone looking for a 30,000 foot view of what constitutes homeland security can benefit from spending time with it.

The book is primarily descriptive rather than evaluative. The authors write that the content is designed to support the (unspecified) "learning objectives established by the programs and guidelines of the Department of Homeland Security and the United States Citizens Corps." [xvii] I have searched unsuccessfully for those learning objectives. I presume they exist; I just cannot locate them.

The authors quickly dismiss any potential conflict over the scope of homeland security by pragmatically noting: "The U.S. government defines homeland security as the domestic effort...to defend America from terrorists. In practice, homeland security efforts have also come to comprise general preparedness under the all-hazards doctrine...." [xiv] Not a lot of academic parsing of ideas here; just a straight forward, "Here are the initial conditions; we can argue details later."

The book is extremely well organized for an undergraduate class in homeland security. Each of the eighteen chapters follows the same format: an overview of the chapter, the learning objectives, the content, a summary of the content, a brief quiz that can also be used as discussion questions, and references. The chapters, generally more broad than deep, introduce readers to most of the topics that can be said to constitute a strict constructionist view of homeland security – i.e., homeland security is about terrorism. The helpfully descriptive chapter titles give one a sense of the breadth of the book:

Part 1 – How We Got Here From There: The Emergence of Modern Homeland Security

- Homeland Security: The American Tradition
- The Rise of Modern Terrorism: The Road to 9/11
- The Birth of Modern Homeland Security: The National Response to the 9/11 Attacks

Part 2 – Understanding Terrorism

- The Mind of the Terrorist: Why They Hate Us
- Al-Qaeda and Other Islamic Extremist Groups: Understanding Fanaticism in the Name of Religion
- The Transnational Dimensions of Terrorism: The Unique Dangers of the Twenty-First Century
- Domestic Terrorist Groups: The Forgotten Threat
- Terrorist Operations and Tactics: How Attacks are Planned and Executed
- Weapons of Mass Destruction: Understanding the Great Terrorist Threats and Getting Beyond the Hype
- The Digital Battlefield: Cyberterrorism and Cybersecurity

Part 3 – Homeland Security: Organization, Strategies, Programs, and Principles

- Homeland Security Roles, Responsibilities, and Jurisdictions: Federal, State and Local Government Responsibilities

- America's National Strategies: The Plans Driving the War on Global Terrorism and What They Mean
- Domestic Antiterrorism and Counterterrorism: The New Role for States and Localities and Supporting Law Enforcement Agencies
- Critical Infrastructure Protection and Key Assets: Protecting America's Most Important Targets
- Incident Management and Emergency Management: Preparing For When Prevention Fails
- Business Preparedness, Continuity, and Recovery: Private Sector Responses to Terrorism
- Public Awareness and Personal and Family Preparedness: Simple Solutions, Serious Challenges
- The Future of Homeland Security: Adapting and Responding to the Evolving Terrorist Threat While Balancing Safety and Civil Liberties

Appendices

- Profile of Significant Islamic Extremist and International Terrorist Groups and State Sponsors
- Volunteer Services
- The Media and Issues for Homeland Security
- Medical and Public Health Services Emergency and Disaster Planning and Response: Public Health and Medical Organizations Have Unique and Demanding Responsibilities for Preparing and Responding to Terrorist Attacks
- Preparing and Responding to Threats Against the Agriculture Sector

The book can be criticized on several grounds. It is largely federal centric, and downplays the role of state and locals in intelligence and other homeland security domains; as described above, some of its content has been overtaken by events – changes in catastrophic planning, changes in the intelligence community, and so on. It could be significantly more critical of existing homeland security orthodoxy, or at least present some conflicting perspectives. It would benefit from a bibliography. There could be links to more current on-line material. But praise for this book should be louder than disdain. Parts I and II have lasting value. It is friendly to students and teachers. It covers a lot of ground.

As yet there is no standard homeland security text book. One day there will be. I consider the Sauter and Carafano book essential because it illustrates what a good introductory homeland security textbook should have: broad coverage to show the scope of the field, clear and informative writing, specific learning objectives, and activities that can be used to determine whether those objectives have been achieved.

The essential character of this book rests not so much in its content but in its structure and presentation. There may be better introductory textbooks in the future. This is the one they will have to surpass.

### *Catastrophe, Preparation and Prevention for Law Enforcement Professionals*, by Craig Baldwin, Larry Irons, and Philip Palin[19]

The previously mentioned book is for people who want to understand the issues and ideas in homeland security. *Catastrophe, Preparation and Prevention* is intended more for people who want to know what to do with those ideas. The book (workbook, actually) is designed for practitioners, especially those at state and local levels. While this book is written primarily for law enforcement, it would be useful for practically any public safety first responder who has some homeland security involvement. It is, according to the material in the book, the first in a series of similar workbooks for fire services, emergency medical, and others.

Prevention is the first priority of the national strategy for homeland security. But what does one do when one is preventing terrorism? As of yet, there is no national strategy for prevention, unlike the ones for response or for protecting critical infrastructure. This book describes a set of principles that can be used to prevent or mitigate a catastrophic attack in one's community. The workbook is based on a prevention model first developed by DHS in its 2003 prevention guidelines.[20] The model was derived inductively by asking first responders what they do when they prevent certain kinds of terrorist attacks. The research generated five general prevention areas: identifying threats, sharing information, collaborating with others, managing risks, and then intervening.

Building on this model, the 150 page workbook seeks to teach police officers the basics of prevention. The book is visually appealing; its content is part theory, part practice, and part fill-in-the-blanks with one's own experiences. The book comes with a compact disk that contains dozens of homeland security documents.

The book is also linked to an on-line exercise where the reader gets the opportunity to test his or her skill in relation to what is taught in the book. For example, after completing the unit on recognizing threats, the reader is directed to the exercise with the following directions:

> It is now 9 months before a planned terrorist attack. The threat is organizing, planning and becoming real. Can you identify the most probable targets [in the fictional community used in the exercise] and their vulnerabilities based on the perceived threat? ....Your efforts to collaborate and share information are paying off. You are receiving information from local, federal and international law enforcement agencies. But, even with this information, you must make threat and vulnerability choices. [46]

After the chapter on risk management, the exercise progresses: "It is now about 3 months before the attack.... You and your team are ready to identify and assess the risks associated with this threat.... Three... lieutenants will present their risk management strategies. Can you correctly identify their strength and weaknesses?" [116]

It all sounds a bit contrived, but from a learning perspective it seems to work. I went through the on-line exercise and learned something about prevention.

(Disclosure: I participated on a review board for McGraw Hill when it was considering whether to undertake this workbook, and I participated in helping to develop one of the concepts used in the workbook. A company I have a relationship with has the potential to benefit financially, in a minor way, from sales of the workbook. These facts normally should exclude someone – in this case me – from writing a review about the book. In spite of that, I still think this workbook demonstrates an important blended learning approach to practitioner-oriented homeland security education.)

One can disagree with some of the conceptual choices made by the authors – in their framing of the prevention equation, for example, or in their focus on terrorism rather than all hazards. I disagree with their use of "decide to intervene" rather than "intervene." But I think this book is essential in the way it approaches practitioner learning. Documents from the national strategy on down, and leaders from the president on down, have talked about prevention as the first priority in securing the homeland. This workbook is the only book I know that treats that priority in a serious and operationally useful way. In doing so, it sets a mark that future efforts to teach practitioners will have to reach.

### *Trapped in the War on Terror*, by Ian S. Lustick

The War on Terror itself, not al Qaeda or its offshoots, "has become the primary threat to the well-being of Americans in the first decade of the twenty-first century. My fundamental conclusion is that the War on Terror is vastly out of proportion to the actual problems we face from terrorists and terrorists groups." [6] *Trapped in the War on Terror*[21] details how Ian Lustick reached this conclusion. He asserts:

> The War on Terror's record of failure, with its inevitable and spectacular instances of venality and waste, will humiliate thousands of public servants and elected officials, demoralize citizens, and enrage taxpayers. The effort to master the unlimited catastrophes we can imagine by mobilizing the scarce resources we actually have will drain our economy, divert and distort military, intelligence, and law enforcement resources, undermine faith in our institutions, and fundamentally disturb our way of life. In this way the terrorists who struck us so hard on September 11, 2001, can use our own defensive efforts to do us much greater harm than they could ever do themselves. [ix-x]

It takes Lustick 145 pages to unfurl compelling – if occasionally polemical and not always thoroughly convincing – evidence to support his assertion. He begins by describing the role triage ought to play in deciding how to use scarce homeland security resources. "If we do not systematically evaluate threats, we will end up worrying about all conceivable

vulnerabilities. By this logic, our resources will be the only limit to investments in our security, leading to a frenzy of impossibly huge outlays." [3]

Lustick argues we do not have an effective way to determine which potential threats are serious enough to attend to. What he calls an "all-azimuth threat of terrorism" makes it difficult to reject rationally any suggestion for being better prepared. There is always something more one can do to prevent or get ready for an attack. One is always open to criticism after the fact if one knew about a potential threat yet did nothing about it. He offers a more conspiratorial explanation that the all-azimuth vision results from the "paranoia unleashed after the 9/11 attacks" that is being exploited by certain special interest groups and individuals. The latter explanation constitutes a significant part of his argument (as Lustick's essay elsewhere in this issue outlines). The bulk of the book is a well structured argument that looks at the causes and consequences of the homeland security world he sees. He closes his analysis with seven ideas he thinks can "free Americans from the War on Terror."

Chapter 2, "Perceptions of the Terrorist Threat" discusses what Americans believe about the threat of terrorism and why they hold those beliefs. Chapter 3 looks at the evidence of the supposed threat. Lustick concludes that there is "very little evidence, hard or soft, that 'terrorist groups with global reach' are operating in the United States with plans to use deadly force either catastrophically or non-catastrophically in attacks against American targets." [29] Lustick does not contend there is no threat [46]. He argues the threat is – in the words of another book that makes a similar point – "overblown." [22]

Lustick uses Chapter 4 to explain why the War on Terror is out of hand.

> The array of slogans, bureaucracies, lobbying strategies, wars, budgets, contracts, books, television shows, films, cottage industries, and academic centers that makes up the War on Terror has come to operate as a self-organizing, self-perpetuating whirlwind – a veritable hurricane of public policies and private ambitions that feed on one another and on the impossibility of any outcome we could know as 'victory.' [48]

He blames the "actions of a very specific, energetic, well-organized, and well-positioned group" for transforming "the national response to the 9/11 attacks from a rational and direct action" against al Qaeda "to a crusade for the implementation of its own long-cherished blueprint for a new kind of America and a new kind of American role in the world." [49]

Chapter 5 describes the War on Terror Whirlwind. Lustick argues we are in what seems to be a permanent national emergency. We have been at threat level Yellow since the advisory system started; airports remain at Orange. The perceived emergency has engulfed the country in a whirlwind of homeland security activities, "none of which can ever be proven successful, but all of which can be criticized as inadequate." [71] He

contends "chasing dollars and grinding axes" drives the whirlwind. Organizations are more likely to receive government funding if they can frame their interests and mission within a homeland security context. District attorneys, veterinarians, the pharmaceutical industry, pediatricians, psychologists, pro-gun groups, anti-gun groups, airlines, unions, insurance companies, housing groups, and a growing list of other special interests assemble what they believe to be credible rationales for a nexus with homeland security.

How do we get free of this trap? Lustick's first recommendation is to know the enemy and then structure our response around that knowledge. "Our enemies are clever and they know more about us than we do about them," he argues. [140] "We must ask the same questions about al Qaeda and its ilk that we would ask about any other opponent." [125] Like Scheuer, he has his own understanding about the enemy, drawn mostly from what they say.

Once we know the enemy, what is to be done? Lustick closes his book with seven suggestions:

1. Open up a debate about the logic and appropriateness of the War on Terror. He notes that polls typically do not ask the American people whether we should have a War on Terrorism. He believes it will be difficult to get this conversation started.
2. Treat terrorists as "the dangerous but politically insignificant criminals they would be without our help." [137]
3. Treat terrorism fundamentally as a law enforcement problem; address the problem with "well-funded, sustained, disciplined, professional, aggressive, internationally cooperative...efforts employed to pursue, prosecute, and punish criminals." [139]
4. Work, long term, to build societies that are sufficiently satisfying and resilient to mitigate the growth of terrorism.
5. Establish levels of acceptable terrorism risks, using reasonable and cost effective measures to reduce unacceptable risks.
6. Learn to manage the fear terrorism seeks to create. "Stare straight into the face of the possibility that our country could be hit by a nuclear [or other catastrophic] terrorist attack," he says. [144] But "remember that we can and will recover from such a blow."[145]
7. "Choose the leaders we deserve, not only to escape the War on Terror trap but to protect ourselves from the real threats we face." [145]

Is Lustick correct? Have we created a self organizing monster that continues to grow and consume ever more resources? The Department of Homeland Security's budget is one of the few domestic policy budgets that are growing. Why is that? Is the threat so immediately malignant that we need to remain on full alert? Are our vulnerabilities so broad and

menacing that we need to continue spending regardless of the costs it imposes on policy domains not connected to homeland security? We have been at this homeland security business for more than five years. Lustick responsibly asks whether we are on the right path. People seriously thoughtful about the security of the American homeland need to engage his argument with equal care.

### *Unconquerable Nation*, by Brian Jenkins[23]

*Unconquerable Nation* combines into one volume some of homeland security's best writing, scholarship, history, critical thinking, pragmatism, personal opinion, and political acumen. The book draws its title – and its central analytical premise – from one of Sun Tzu's less well-known aphorisms: "Being unconquerable lies with yourself."

"Let us keep the threat in perspective," Jenkins argues (although not as zealously as Lustick). "We have in our history faced far worse threats. Our lives are not in grave danger. The republic is not in peril. We must not overreact." [177]

Like Scheuer, Flynn, and others, Jenkins argues that our strategy in the struggle against terrorism

> [M]ust be based on a thorough understanding of the enemy and of one's own strengths and weaknesses. 'Being unconquerable' means knowing oneself, but as understood by the ancient strategists, 'knowing' means much more than the mere acquisition of knowledge. 'Knowing oneself' means preserving one's spirit, a broad term. 'Being unconquerable' includes not only disciplined troops and strong walls, but also confidence, courage, commitment—the opposite of terror and fear. [5]

Jenkins – who has been involved in terrorism research for almost forty years – believes we can successfully defeat the threat of terrorism and preserve our liberty and our values. He argues that

> [T]oday's fierce partisanship has reduced national politics to a gang war. The constant maneuvering for narrow political advantage, the rejection of criticism as disloyalty, the pursuit by interest groups of their own exclusive agendas, and the radio, television, newspaper, and Internet debates that thrive on provocation and partisan zeal provide a poor platform for the difficult and sustained effort that America faces. All of these trends imperil the sense of community required to withstand the struggle ahead. We don't need unanimity. We do need unity. Democracy is our strength. Partisanship is our weakness. [17]

The book is about terrorists and homeland security. The first two chapters review the progress of the terrorism wars from the immediate post-9/11 days through current insurgent activities in Iraq.

> It is evident that this conflict will not be decided in the near future but will persist...for decades, during which setbacks will be

> obvious and progress will be hard to measure. Beyond al Qaeda, we confront a protracted ideological conflict, of which the terrorist campaign waged by disconnected jihadists is a symptom.... Preparing for this long war will require a deeper understanding of the challenge we confront and the formulation of a set of strategic principles to guide our actions. [51]

Identifying these principles for both the international and domestic fronts is the heart of Jenkins' book.

Chapter Three is another effort to "know the enemy." The terrorism debate is shaped on the one hand by seeing the enemy easily as evil people who hate our way of life and on the other by a more complex view of an enemy with clear foreign policy objectives. Jenkins writes, as did Scheuer and Lustick, "If you want to know what enemy leaders are thinking about, listen to what they have to say." [61]

Jenkins reviews some of the common misperceptions about the enemy, and then focuses on their words. One intriguing feature of the chapter is an analysis of the jihadist ideology and three generations of jihadist leaders. He concludes that

> [The jihadist] words are a narrative aimed at the home front, intended above all to incite action. They convey a message that has resonance and undeniable appeal. .... [T]he jihadists' actions are aimed at maintaining unity and attracting more recruits.... This fight will go on for a long time, especially if we fail to see it through their eyes. But once we do, we can formulate a new set of strategic principles better suited to the conflict. [109]

Another section especially worth reading is a hypothetical briefing given to Osama bin Laden about how al Qaeda and the jihad are doing, five years after the attack on American soil.

Chapter Four outlines the principles Jenkins suggests should govern our approach to this struggle. They include destroying the global jihadist enterprise, conserving resources for a decades long war, waging the political war against the jihadist ideology more effectively, breaking the cycle of jihadism, maintaining international cooperation, maintaining a narrower view of preemption, and reserving the right to retaliate (massively if necessary) in response to an attack.

Chapter Five presents the implications of Jenkins' argument for homeland security. The chapter opens with a unique photographic image of the Statue of Liberty and the torch she holds in her right hand. Under the picture are the words "The defense of democracy demands the defense of democracy's ideals."

Like Lustick, Jenkins asks: how did America become so afraid?

> Fear is the biggest danger we face. Fear can erode confidence in our institutions, provoke us to overreact, tempt us to abandon our values. There is nothing wrong with being afraid, but we have spent

> the past five years scaring the hell out of ourselves. We need to spend the next several years doing things very differently. [153]

His suggestions about what to do differently are not especially new. Yet they add to a growing perception that we know we can be doing better in homeland security. But the political will to make those changes happen has yet to emerge.

Jenkins recommends getting realistic about risk: "Since 9/11, most Americans have exaggerated the danger posed by terrorist attacks. This is because spectacular events, not statistics, drive our perceptions."[154] He adds his voice to those who want to get citizens more actively involved in preparedness activities:

> The federal government does not provide homeland security. Citizens do.... Security is a fundamental human right, but it should not become an individual entitlement. Americans are going to have to accept a measure of risk, even if the risk is minuscule, as we have seen. Yet the acceptance of risk should never become an excuse for negligence. [158]

Accomplishing this aim, as Jenkins describes it, will require more than an inadequately funded Citizen Corps.

His other recommendations include becoming more sophisticated about security, about what it can and cannot do; favoring security investments that help rebuild the nation's physical and social infrastructure; improving state and local intelligence capabilities; building a better legal framework to improve our ability to prevent attacks while respecting civil liberties; and ensuring effective judicial and legislative homeland security oversight.

Jenkins' final principle for redirecting homeland security efforts is to preserve American values. One often hears that the Constitution is not a suicide pact.[24] Jenkins confronts that concern:

> Maintaining our values may at times be inconvenient. It may mean, in some circumstances, accepting additional risks, but America has fought wars to defend what its citizens regard as inalienable rights. The country has faced dangers greater than all of the terrorists in the world put together. Neither the terrorists nor those who would promise us protection against terror should cause us to compromise our commitments. The current campaign against terrorism is a contest not only of strength and will, but also of conviction, commitment, and courage. It will ultimately determine who will live in fear. The choice, ultimately, is our own. I believe that we can win, and we can win right. [176]

The sentiment Jenkins expresses is essential to homeland security.

Jenkins argues that our most effective defense against terrorism will come from "our own virtue, our courage, our continued dedication to the ideals of a free society." [176] My final candidate for essential homeland security

work is a trinitarian reminder of what those ideals are: ***The Declaration of Independence, The Articles of Confederation,* and *The Constitution of the United States of America.***

The *Declaration of Independence* asserts, without providing footnotes, citations or other supporting evidence, that certain truths are self-evident: "that all Men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty, and the Pursuit of Happiness – That to secure these rights Governments are instituted among Men.... " But when government "becomes destructive of these Ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its Foundation on such Principles, and organizing its Powers in such Form, as to them shall seem most likely to effect their Safety and Happiness."

Our nation's roots spring from a revolution against illegitimate authority. But we have come a long way from Patrick Henry's "Give me liberty or give me death" to the unquestioning acceptance of "You are required to remove your shoes before you enter the walk-through metal detector."[25]

The *Declaration* reminds us that government's authority is derived from the consent of the governed. Governments take silence as consent. More people voted in 2006 for *American Idol* than have ever voted for a president.[26] The right combination of issue, incident, fear, and demagogue could radically alter the kind of nation we pass on to our children. If we perceive our safety is in jeopardy, we can change our laws. The rapid passage of the 300 plus page USA PATRIOT Act in 2001 – signed six weeks after the 9/11 attacks – demonstrated government can act quickly, more quickly than the Founders envisioned. New laws can enshrine new "self-evident" values.

I included the *Articles of Confederation And Perpetual Union* as a fundamental homeland security document because it reminds us that we did not get it right the first time we tried to form a government. We can make, acknowledge, and correct error.

The *Articles* were written during the war in 1776, adopted in 1777, and ratified by the states in 1781. This pact of Perpetual Union did not attend to the practical realities of financing and administering a nation. Instead of continually trying to modify the *Articles* until they got it right, the Founders had the political courage to start over again. The *Articles of Confederation* remind us that we should not exclude the possibility of rethinking, as a nation, how we approach homeland security. There are strong arguments to be made that the practice of homeland security is unnecessarily large and overly complex for the actual task we face. According to that perspective, expenditures are precariously out of balance with the threat. Our current confederation of homeland security activities risk – as bin Laden predicted in his October 2004 videotape – "continuing this policy in bleeding America to the point of bankruptcy." [27]

The *Constitution of the United States* – and the more than 200 year history of interpreting that document – is, and ought to provide, the foundational understanding of what it means to participate in this nation. Samuel Adams wrote:

> The liberties of our country, the freedoms of our civil Constitution are worth defending at all hazards; it is our duty to defend them against all attacks. We have received them as a fair inheritance from our worthy ancestors. They purchased them for us with toil and danger and expense of treasure and blood. It will bring a mark of everlasting infamy on the present generation – enlightened as it is – if we should suffer them to be wrested from us by violence without a struggle, or to be cheated out of them by the artifices of designing men.

The *Constitution* reminds us that our continually emerging, perpetually incomplete, task is to form a more perfect union, establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare, and secure the blessings of liberty. Those are essential principles around which to secure the American homeland.

*Christopher Bellavita teaches at the Naval Postgraduate School in Monterey, California. An instructor with twenty years experience in security planning and operations, he serves as the director of academic programs for the Center for Homeland Defense and Security. He received his PhD from the University of California, Berkeley.*

---

[1] National Commission on Terrorist Attacks Upon the United States, *The Final Report of the National Commission on Terrorist Attacks Upon the United States: 9/11 Commission Report* (New York, NY: Barnes & Noble Publishing, Inc., 2004).

[2] In 1973 the report on the prison uprising at the Attica State Correctional Facility in upstate New York was one of the award finalists. Neither report won.

[3] Richard A. Posner, "The 9/11 Report: A Dissent," *New York Times*, August 29, 2004.

[4] Department of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: U.S. Government Printing Office, 2002).

[5] Henry Mintzberg, Joseph Lampel, and Bruce Ahlstrand, *Strategy Safari: A Guided Tour through the Wilds of Strategic Management* (New York, NY: Free Press, 1998).

[6] Christopher Bellavita, "Changing Homeland Security: Shape Patterns, Not Programs," *Homeland Security Affairs* II, no. 3 (October 2006): 1, http://www.hsaj.org/?article=2.3.5.

[7] Richard A. Falkenrath,"Homeland Security: The White House Plan Explained and Examined," Paper presented at the Brookings Forum, The Brookings Institution, September 4, 2002, 6.

[8] Ibid., 4.

[9] Colin S. Gray,"Why Strategy Is Difficult," *Joint Forces Quarterly* (1999), 9.

[10] Falkenrath, "The White House Plan," 4.

[11] Steven Brill, *After: How America Confronted the September 12th Era* (New York, NY: Simon & Schuster, 2003).

[12] Author's conversation with Mr. Darrell Darnell, June 2004.

[13] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press), 275; as quoted in John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them* (New York, NY: Free Press, 2006), 9.

[14] Michael Scheuer, *Imperial Hubris* (Dulles, VA: Brassey's Inc., 2004).

[15] Stephen Flynn, *America the Vulnerable: How Our Government Is Failing to Protect Us from Terrorism* (New York, NY: HarperCollins, 2004).

[16] Stephen Flynn, *The Edge of Disaster* (New York, NY: Random House, 2007).

[17] Flynn, *American the Vulnerable*, 145ff

[18] Mark A. Sauter and James Jay Carafano, *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism* (New York, NY: McGraw-Hill, 2005).

[19] Craig Baldwin, Larry Irons, and Philip J. Palin, *Catastrophe Preparation and Prevention for Law Enforcement Professionals* (New York, NY: McGraw Hill, 2008).

[20] U.S. Department of Homeland Security, *Preparedness Guidelines for Homeland Security* (Washington, DC: Office for Domestic Preparedness, June 2003).

[21] Ian S. Lustick, *Trapped in the War on Terror* (Philadelphia, PA: University of Pennsylvania Press, 2006).

[22] John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them* ( New York, NY: Free Press, 2006). Lustick's and Mueller's point was illustrated recently in Dan Eggen, "Justice Dept. Statistics On Terrorism Faulted; Most Numbers Inaccurate, Audit Shows," *Washington Post*, February 21, 2007, Page A08. http://www.washingtonpost.com/wp-dyn/content/article/2007/02/20/AR2007022001566.html

[23] Brian Michael Jenkins, *Unconquerable Nation: Knowing Our Enemy; Strengthening Ourselves* (Santa Monica, CA: RAND, 2006).

[24] "This Court has gone far toward accepting the doctrine that civil liberty means the removal of all restraints from these crowds and that all local attempts to maintain order are impairments of the liberty of the citizen. The choice is not between order and liberty. It is between liberty with order and anarchy without either. There is danger that, if the Court does not temper its doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact." http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=337&invol=1 (Terminiello v. City of Chicago). For an analysis of how this phrase has been used see David Corn, "The 'Suicide Pact' Mystery: Who coined the phrase? Justice Goldberg or Justice Jackson?" January 4, 2002, http://www.slate.com/id/2060342/.

[25] http://www.tsa.gov/travelers/airtravel/assistant/shoe_screening.shtm

[26] In May 2006, 64 million people voted in the American Idol final; in 1984, 54.5 million people – the most ever – voted for Ronald Reagan in the 1984 presidential election. A total of 92.5 million votes were cast in the 1984 election. See "American Idol Outvotes the President," *The Guardian*, May 26, 2006. http://www.guardian.co.uk/international/story/0,,1783339,00.

[27] http://english.aljazeera.net/news/archive/archive?ArchiveId=7403

# Fractured Fairy Tale: The War on Terror and the Emperor's New Clothes

Ian S. Lustick

*A version of this article is also appearing in the Minnesota Journal of International Law.*

## THE INVISIBLE IRRATIONALITY OF THE WAR ON TERROR

The War in Iraq has become politically radioactive. It is a burden, not a boon, to any politician associated with it. Not so the War on Terror. It continues to attract the allegiance of every politician in the country, whether as a justification for keeping U.S. troops in Iraq (to win the "central front" in the War on Terror), or as a justification for withdrawing them (to win the really crucial battles in the War on Terror at home and in Afghanistan). Both official rhetoric and practice, including wars abroad, massive surveillance activities, and colossal expenditures, have bolstered the reigning belief that America is locked in a death struggle with terrorism. Since 2001 the entire country, every nook and cranny, has been officially deemed to be exposed to at least an "elevated" risk of terrorist attack—"Threat Condition Yellow"—with episodes and particular locations sometimes labeled as Orange, meaning "severe" risk of terrorist attack. By mid-2006 the United States had spent at least $650 billion on the War on Terror, including expenditures linked to the wars in Afghanistan and Iraq. In the three years between October 2002 and October 2005, high-ranking Department of Defense officials gave 562 speeches with some version of the word “terror” in their titles. That means they gave 36 percent more speeches about terrorism than about Secretary of Defense Rumsfeld’s signature theme (transformation of the military), twenty-two times more speeches about terrorism than about nuclear weapons, forty-three times more than about proliferation, and fifty-one times more than about ballistic missile defense.[1]

What is true of the government and of politicians is also true of the American public, which seems convinced of the potency of the threat and the necessity of the war. Five years after the 9/11 attacks, and despite the absence of attacks since then or of any evidence of serious preparations for an attack inside the country, 76 percent of Americans responded affirmatively to a *New York Times/CBS News* poll that asked whether they believed "...the terrorist threat from Islamic fundamentalism is constantly growing and presents a real, immediate danger to the United States, or not?" Sixty percent said they thought the United States should do more to try to prevent further terrorist attacks. Seventy-four percent said they were "somewhat" or "a great deal" concerned about the possibility that there will be major terrorist attacks in the United States (up from 71 percent three years earlier). Thirty-five percent said they were somewhat or a great deal worried that such an attack would harm them personally (a level of worry that has remained more or less constant since 2001).[2] As instructive as these answers to polls are, even more enlightening are the questions. Of the scores, probably hundreds, of polls done regarding the prosecution of the War on Terror, how it should be conducted, how well the government is doing, how important to it is

the Iraq War, how much more should be done in it, it is difficult, indeed, impossible to find a survey by a major American polling organization that has even asked the question, "Do you think there should be a War on Terror?"

Of course popular perceptions are not molded or sustained only by the speeches and actions of government officials and politicians, nor only by the narratives and assumptions of the news media – though the news media has been a major cheerleader for the War on Terror. The entertainment industry, in novels, television shows, films, and made-for-television movies has hyped the fears that fuel the War on Terror and keep it alive. Thus has the War on Terror embedded itself into popular culture. Both Hollywood and the television networks have plunged aggressively into the preparation and distribution of films and television dramas depicting threats of catastrophic terrorism. These have included the film *The Sum of All Fears*, featuring the destruction of Baltimore by a nuclear bomb smuggled into the country by terrorists; *Face of Terror*, about a Palestinian terrorist bomber in Spain; *Antibody,* about an international terrorist with access to a nuclear detonator; *American Heroes: Air Marshal*, about a jetliner hijacked by terrorists with ambitious plans; *When Eagles Strike*, about terrorists who kidnap an American senator; and *Blast!*, about terrorists who take over an oil rig to detonate an electro-magnetic bomb over the United States. A quick survey of a bookstore in Philadelphia International Airport in the summer of 2005 revealed that of thirty-five paperback novels for sale to travelers waiting to board their planes, seven shared fundamentally the same plot – imminent disaster at the hands of maniacal terrorists that might still be thwarted by courageous counter-terrorist action. These 20 percent included Tom Clancy's *Splinter Cell*, Michael Crichton's *State of Fear*, Dan Brown's *Deception Point*, James Patterson's *London Bridges*, and Robert Ludlum's the *Lazarus Vendetta*.

Made-for-television movies on these themes were also plentiful. These included *Winds of Terror* (2002), about a biological weapon attack on the United States; *Operation Wolverine: Seconds to Spare* (2003), about terrorists hijacking a train to release enough poison gas to destroy a large American city; *The President's Man 2: A Line In the Sand* (2002), about a secret agent's effort to foil terrorists constructing a nuclear weapon; *Smallpox 2002: Silent Weapon* (2002), about a bioterrorist smallpox attack; *The Pilot's Wife* (2002), about the terrorist bombing of a 747 airliner; *Counterstrike* (2003), about terrorists with a nuclear weapon who hijack the Queen Elizabeth II luxury liner; *Critical Assembly* (2003) in which a nuclear bomb produced by students is stolen by terrorists; and *Tiger Cruise* (2004), about a navy ship's reaction to the 9/11 attacks. Of all the made-for-television movies and theatrical releases dealing with terrorist themes in recent years, however, there is probably no movie that has had a wider viewership than *Dirty War* (2004), an extremely realistic docudrama depicting Middle Eastern terrorists who detonate a radioactive "dirty bomb" in London. Produced by the BBC and originally aired in Britain, the film was then delivered to HBO in the United States, which broadcast it repeatedly in early 2005.

During the regular viewing seasons of the past few years, television viewers have been treated to half a dozen new shows about terrorism and/or specialized military, intelligence, and law enforcement agencies fighting terrorists. These programs have included: *The Agency* (CBS); *NCIS* (CBS); *Threat Matrix* (ABC);

*Alias* (ABC); *The Unit* (CBS); and, most popular of all, "*24*" (Fox). The entire 2005 season of *24* was devoted to a story line involving a sleeper cell of Middle Eastern terrorists in the United States that unleashes a nuclear-tipped missile against a major American city.[3] In December 2005 the Showtime cable channel presented a miniseries about Islamic terrorists in the United States entitled *Sleeper Cell*. As Michael Ealy, the star of the show, put it, "This show is about the reality of the Beast that we're fighting right now, on many fronts."[4] A continuation of the *Sleeper Cell* series aired in December 2006.

What accounts for the prominence of the terrorist threat in the American imagination and the stupendous success of the War on Terror as a political program, frame of reference for policy? Certainly it is not the scale of the threat to the homeland. Since 9/11 there has been no evidence of any serious terrorist threat from Islamic extremists inside America, no sleeper cells, no attacks, no serious planning or preparation for an attack. Major university studies have reported that 90 percent of all cases presented for prosecution to district attorneys by the FBI or other law enforcement agencies have been rejected as lacking sufficient evidence to proceed with prosecution. In the two years after the 2001 attacks the median sentences handed out to those found guilty under the terrorism laws was twenty-eight days. In the subsequent two years the median sentence for those (few) found guilty has been twenty days. These figures reflect the fact that the great majority of these prosecutions are not really for terrorism offenses, but for telling untruths to law enforcement officers, visa violations, and the like.[5]

The absence of terrorist activities in the United States is all the more striking in light of three other considerations. First, "red-team" exercises, designed to test the effectiveness of anti-terrorism precautions against determined adversaries, regularly show how easy it would be for a motivated and minimally resourced terrorist to circumvent most measures that have been (or could be) put in place. Second, monthly (if not weekly) shootings in schools, malls, and office buildings show how easy it would be for terrorists bent simply on killing Americans to do so. Third, the absence of very many successful prosecutions is even more compelling evidence than it otherwise would be of the virtual absence of a serious domestic terrorist threat because of the unprecedentedly exhaustive, constant, unrestrained, and heavily funded scrutiny of anyone American law enforcement agencies have had even the vaguest reason to suspect and to the government's adoption of a general posture of "pre-emptive prosecution."[6] For all these reasons, many Americans, including high-ranking officials and analysts, have found the absence of attacks to be truly puzzling.

At the end of this essay I will return to the question of al-Qaeda's motives as a partial answer to this puzzle. However, what has puzzled me more than the failure of al-Qaeda and its clones to attack again since 2001 is the related question of how, in the absence of evidence of a threat, to explain the War on Terror. What accounts for nearly universal allegiance of American interest groups to the War on Terror, the steady polling numbers showing support for it, the often panicky concern that it is not being prosecuted successfully enough, its dominance of the political landscape, and the $650 billion that we have so far

spent on it? Answering these questions means understanding how the War On Terror was triggered, how it sustains itself, and how it conceals its irrationality.

## The War in Iraq and the War on Terror

The official mantra is that we fight in Iraq because it is the "central front in the War on Terror." The exact opposite is the case. We are trapped in fighting an unwinnable and even nonsensical "War on Terror," *because* its invention was required in order to fight in Iraq. When we were struck on September 11, 2001, the U.S. military budget was the equal of the military budgets of the next twenty-four most powerful countries. That structural fact of military uni-polarity, by sharply reducing the perception of the costs of military adventures, made it likely that the United States would fight some kind of war abroad. However, in the first eight months of the George W. Bush administration pragmatists in the State Department, the uniformed military, and the intelligence community checked efforts by the Project for the New American Century-inspired and Cheney-Rumsfeld led supremacist cabal to launch a war in Iraq as the first stage of a radical transformation of U.S. foreign policy toward global American hegemony and military unilateralism.[7] However, when 9/11 produced an immense amount of political capital for a President peculiarly ready to accept the role offered him by the cabal, of anointed Churchillian savior in a global, epochal, "War on Terror," the cabal had exactly what it needed. As they spun it, the global war on terror divided the world into "those with us versus those against us." Coupled with the principle of pre-emption, this radical division of the world, into our camp and the enemy camp, rendered automatically any country or group not "with us" as subject to attack by the U.S., at will. Thus, although Iraq had absolutely nothing to do with 9/11, the cabal was able to devise and implement a formula linking the September 2001 attacks to its long-cherished goal – forcible regime change in Iraq as a model for a series of quick, neo-imperialist wars to revolutionize American foreign policy and thereby to serve conservative political objectives at home. Thus the latent propensity of the U.S. to go to war, born of immense military preponderance, was exploited by the cabal, who were able to portray their long sought invasion of Iraq as a requirement of a global War on Terror.

The organizational centerpiece for the activities of this group before 2001 was the Project for the New American Century (PNAC) whose chairman, William Kristol, is also editor-in-chief of the *Weekly Standard*, the magazine universally regarded as the neoconservative movement's mouthpiece.[8] William Kristol and Robert Kagan published an informal manifesto of the PNAC in the Council on Foreign Relations' journal *Foreign Affairs* in the summer of 1996. "Conservatives," they warned, "will not be able to govern America over the long term if they fail to offer a more elevated vision of America's international role." The role they described for the United States was to establish a position of "benevolent global hegemony" and to preserve it "as far into the future as possible." The dual purpose of the muscular use of American hyper-power would be "to destroy the world's monsters" and to "manage empire." To implement this post-Cold War vision, to overcome the electoral advantages of Clinton-style platforms of multilateralism abroad and social democracy at home, Kristol and

Kagan called for "a true 'conservatism of the heart'" that would "emphasize both personal and national responsibility, relish the opportunity for national engagement, embrace the possibility of national greatness, and restore a sense of the heroic." They claimed their "neo-Reaganite foreign policy…would be good for conservatives, good for America, and good for the world….Deprived of the support of an elevated patriotism, bereft of the ability to appeal to national honor, conservatives will ultimately fail in their effort to govern America."[9]

PNAC was the driving force behind Congressional passage of the 1998 Iraq Liberation Act. In January of that year PNAC had delivered a letter to President Clinton demanding war to remove Saddam Hussein's weapons of mass destruction (WMD) and to remove and replace Saddam and his regime as a crucial first step to transforming the Middle East. "We urge," said the letter, "a new strategy that would secure the interests of the U.S. and our friends and allies around the world. That strategy should aim, above all, at the removal of Saddam Hussein's regime from power….[including] a willingness to undertake military action as diplomacy is clearly failing…[T]hat now needs to become the aim of American foreign policy." In addition to the names of many of those who signed the PNAC statement of purpose, and who became high-ranking officials in the George W. Bush Administration (such as Donald Rumsfeld, Paul Wolfowitz, and Elliot Abrams), names on this letter also included Richard Perle (named chairman of the defense policy board), Richard L. Armitage (deputy secretary of state), John Bolton (undersecretary of state for arms control, later ambassador to the United Nations), and R. James Woolsey (former CIA director and member of the defense policy board).[10]

Within a year after the 9/11 attacks, the cabal got what it had sought for so long – a Presidential decision to invade Iraq.[11] Now, however, after years of slaughter in that country, the neoconservative/supremacist fantasy of a series of cheap, fast hegemony-building wars is dead. The War on Terror, however, born of the cabal's need for a justification for the invasion of Iraq that could link it to 9/11, lives on, stronger than ever. The question we are left with, then, is not how did the War on Terror begin, but how did it take on a life of its own and trap the entire political class, and most Americans, into public beliefs about the need to fight a global war on terror as our first priority, even when there is no evidence of an enemy present in the United States?

## Hurricane Osama

We may begin to understand the answer to this question by considering how Congress, state, and local governments responded to the War on Terror. In the summer of 2003 a list of 160 potential targets for terrorists was drawn up, triggering intense efforts by representatives and senators, and their constituents, to find funding-generating targets in their districts. These pressures resulted in ever broader categories for listing what could be construed as potential targets of terrorism. The names of these lists changed rapidly between 2003 and 2005, from "Critical Assets," to "Protected Measures Target List," to "Critical Infrastructure/Key Resource List," to "National Asset Data Base." These widening categories enabled mushrooming increases in the number of "assets" (commonly identified by county governments throughout the country) deemed

worthy of protection: up to 1,849 in late 2003, 28,364 in 2004, 77,069 in 2005, and an estimated 300,000 in 2006 (including the Sears Tower in Chicago, but also the Indiana Apple and Pork Festival).[12]

Across the country virtually every lobby and interest group cast their traditional objectives and funding proposals as more important than ever given the imperatives of the War on Terror. According to the National Rifle Association, the War on Terror means more Americans should carry firearms to defend the country and themselves against terrorists. In April 2002, NRA Executive Director Wayne LaPierre was reported to be celebrating "increased momentum since Sept. 11 for laws permitting concealed guns." After the attacks in September 2001, said LaPierre, "People are unsettled and have a fear of the unknown and of a threat that could come from anywhere, they'd rather face that threat with a firearm than without one."[13] In 2003 the gun lobby announced a new program called NRASafe, described by LaPierre as involving all NRA members in a kind of national neighborhood watch program within the War on Terror. "As freedom's keepers, we cannot be a passive observer in this epic confrontation with evil. I believe this great association has a unique role to play in homeland security. God helps he who helps himself, and nobody knows that better than NRA members. We understand that liberty requires eternal vigilance. Not just as a government, but as a people."[14]

In point of fact, however, the gun lobby had been beaten to the punch by the gun control lobby. Within one week after the 9/11 attacks, gun control lobbying organizations began campaigns linking their long-standing policy preferences for increased restrictions on access to firearms to the need to protect the country against terrorism. An extensive study sponsored by the Brady Center to Stop Gun Violence quoted Bush's November 2001 speech to the United Nations, "We have a responsibility," said the president, "to deny weapons to terrorists and to actively prevent private citizens from providing them." That was all the anti-gun lobby needed to use the War on Terror for its own purposes. As stated in the Brady Center study:

> Terrorists and guns go together. The gun is part of the essential tool kit of domestic and foreign terrorists alike. Guns are used to commit terrorist acts, and guns are used by terrorists to resist law enforcement efforts at apprehension and arrest. The oft-seen file footage of Osama Bin Laden, aiming his AK-47 at an unknown target, is now a familiar reminder of the incontrovertible connection between terrorism and guns.... For terrorists around the world, the United States is the Great Gun Bazaar.[15]

The list of interest groups able to recast their long-sought objectives as imperatives of the War on Terror is virtually endless. Schools of Veterinary Medicine called for quadrupling their funding. Who else would train veterinarians to defend the country against terrorists using hoof and mouth disease to decimate our cattle herds?[16] Pediatricians declared that more funding was required to train pediatricians as first responders to terrorist attacks since treating children as victims is not the same as treating adults.[17] Pharmacists advocated the creation of pharmaceutical SWAT teams to respond quickly with appropriate drugs.[18] Aside from swarms of beltway-bandit consulting firms and huge corporate investments in counter-terrorism activities, universities across

the country created graduate programs in Homeland Security and dozens of institutes on terrorism and counter-terrorism, all raising huge catcher's mitts into the air for the billions of dollars of grants and contracts just blowing in the wind.[19]

As these and other groups found counter-terrorism slogans effective in raising revenue, they became even more committed to the War on Terror, convincing those who had been slow to define themselves as part of the War to do so quickly or lose out. The same imperative – translate your agenda into War on Terror requirements or be starved of funds – and its spiraling consequences, surged across the government, affecting virtually all agencies. Bureaucrats unable to think of a way to describe their activities in War on Terror terms were virtually disqualified from budget increases and probably doomed to cuts.[20] With billions of dollars a year in state and local funding, the Department of Homeland Security devised a list of fifteen National Planning Scenarios to help guide its allocations. To qualify for Homeland Security funding state and local governments had to describe how they would use allocated funds to meet one of those chosen scenarios. What was the process that produced this list? It was deeply political, driven by competition among agencies, states, and localities who knew that funding opportunities would depend on exactly which scenarios were included or excluded – with anthrax, a chemical attack on a sports stadium, and hoof and mouth disease included, but attacks on liquid natural gas tankers and West Nile virus excluded. Most instructive of all, in this process, was the unwillingness of the government to define the enemy posing the terrorist threat. Why? Because once defined, certain scenarios, profitable for some competitors, would be disqualified. Thus the enemy, in these scenarios, is referred to as "the universal adversary;" in other words, as Satan. That is how the War on Terror drives the country, from responding to threats to preparing for vulnerabilities, producing an irrational and doomed strategic posture which treats any bad thing that could happen as a national security imperative.[21]

Of course this entire dynamic is accelerated by the principle of Cover Your Ass (CYA). Each policy-maker knows that if there is another attack, no one will be able to predict where and when it will be, but after it occurs it will be easy to discover who it was who did not approve some project or level of funding that could have prevented it. Every government official is perfectly aware of this asymmetry and perfectly aware also that the most attractive strategy in such a predicament is to endorse whatever option commits more resources to counter-terrorist efforts. In that way, if there is no attack, it can partially be explained by the wise (if expensive) precautionary measures taken. If there is an attack, at least the official who argued for exerting more effort or spending more money will not be blamed for the failure to prevent it.

Another source of energy for the War on Terror whirlwind is competition among politicians. While Karl Rove and company systematically, explicitly, and successfully used accusations of Democrats suffering from a "pre-9/11 mentality" as their weapon of choice in the 2002 and 2004 elections, Democrats were irresistibly drawn to the same slogans. When it was reported that some American ports were to be run, in part, by a company associated with the Arab sheikhdom of Dubai, Democrats fell all over themselves excoriating President Bush for his

obvious incompetence and even, perhaps, his lack of sanity, for making America even more vulnerable to terrorist attack. The absence of any evidence or expert evaluation suggesting that this measure was dangerous had little or no impact on this (successful) Democratic barrage, just as it was the iconic status of the 9/11 Commission, not the actual importance or appropriateness of its analysis and advice, that led Nancy Pelosi to declare that in the first 100 days of a Democratic controlled congress every single one of the 9/11 Commission's recommendations would be fully implemented.

Of course the real beneficiary of such overheated, hyper-politicized argumentation over who is more counter-terrorist than thou is the War on Terror itself. Its status as a national priority to which all politicians *must* pay homage is powerfully reinforced by such competition while its own irrationalities are shielded by an ever thicker protective belt of public catechisms required of any politician to avoid the tag of being "soft" or "pre-9/11" in the War on Terror.

Beyond the activities of lobbyists, interest groups, bureaucrats, corporations, and politicians, there is, however, no more important energy source for the War on Terror than the media. I have already noted the contribution made by a flood of novels, films, and television shows exploiting the thrills of imagined terrorism. But we must also appreciate the direct contribution to the War on Terror made by the news media. Consider what happens when a hurricane or a blizzard bears down on a large American city: the local news media has a field day. Ratings rise. Announcers are barely able to contain their excitement. Meteorologists become celebrities. They warn of the storm of the century. Viewers are glued to their sets. Soon, however, the storm hits and passes, or fizzles and is forgotten. Either way the "storm of the century" story ends. Ratings for local news shows return to normal and anchors shift their attention back to murders, fires, and auto accidents.

When it comes to the War on Terror, however, the "storm of the century," Hurricane Osama, as it were, is always about to hit and never goes away. For the national media this is as good as it gets. The terrorist threat level is always and everywhere no less than "elevated." Absent any actual attacks or detectable threats, government agencies manufacture pseudo-victories over alleged or sting-produced plots to justify hundreds of billions of dollars worth of mostly silly expenditures. With every lost soul captured by the FBI presented as the latest incarnation of Mohammad Atta, the news media and the entertainment industry fairly exults, thriving on fears stoked by evocations of 9/11 and the ready availability of disaster scenarios too varied to be thwarted but too frightening to be ignored. Compounded by media sensationalism, these fears then provide irresistible opportunities for ambitious politicians to attack one another for failing to protect the terrorist target *du jour*: ports, border crossings, the milk supply, cattle herds, liquid natural gas tankers, nuclear power plants, drinking water, tunnels, bridges, or subways. The result of such sensationalist coverage, accompanied by advice from academic or corporate experts anxious to sell their counter-terrorism schemes to a terrified public and a cover-your-ass obsessed government bureaucracy, is another wave of support for increased funding for the War on Terror. But every precaution quickly produces speculation about

work-arounds the terrorists could use, thereby fueling another cycle of anxiety, blame, expert counter-terrorist advice, and increased funding.

These are the vicious circles, the self-powering dynamics, that produce and reproduce widespread hysteria in America over non-existent "sleeper cells" and over our real, but unavoidable, vulnerability to bad things happening – a hysteria not seen here since the anti-communist frenzy of the McCarthy era. It is nothing short of humiliating that the country that was able to adjust psychologically, politically, and militarily to the real capacity of the Soviet enemy to incinerate our cities on a moment's notice has been reduced to moaning, wasting resources, and spinning in circles by ragged bands of Muslim fanatics.

## ESCAPING THE TRAP OF THE WAR ON TERROR

We have been, and are being, suckered, suckered big-time. Before the attacks, al-Qaeda was a shattered remnant of a failed movement, dropping into the dustbin of history, the equivalent of the Aryan Nations on the American political scene. But the diabolical strikes against the twin towers and the Pentagon saved the jihadists. Well, not really. What saved them from political oblivion and lifted them to protagonists, declared as equivalent in potency and world-historic importance to Nazi Germany and Imperial Japan, was the American reaction to those attacks. Our invasion of Iraq, cast within a global War on Terror, was for them the "crusade" that makes their world of "jihad" appear not just real but compellingly real to hundreds of millions of Muslims. The Bush administration launched the War on Terror, but it was a war fought according to Osama's script. Now our army is broken and demoralized in an Iraq War that breeds al-Qaeda recruits and turns their propaganda into reality. Meanwhile the very strength of American democracy and free enterprise – motivating every faction in America to turn the War on Terror to its own interest – is hijacked and turned against us by our adversaries just as effectively as they hit us with our own airplanes on 9/11.

We wanted to arm wrestle with our enemies. Why not? We have more economic and military muscle than any state in history. But that is precisely why they fight us with judo, using our strengths against us. They hijack our planes to attack our buildings. They use our passionate patriotism to propel us in reaction into a war in the Middle East that exactly serves their interests, and was the main reason for their attack. And they hijack Madisonian democracy itself, to create a vortex of aggrandizing exploitation of the War on Terror for self-interested agendas that spin our country out of control.

One of the things that the War on Terror does to defend itself is prevent itself from being known for the Emperor's Clothes phenomenon it fundamentally is. Aside from deterring those politicians and bureaucrats who understand the spectacular irrationality of the War on Terror from saying as much, the truth about its dynamics are concealed by suppressing knowledge of the real attributes, plans, capabilities, and aspirations of al-Qaeda. If we knew and understood al-Qaeda and Osama bin-Laden properly, we would understand that a "War on Terror" is exactly not how we can combat that threat. For example, almost no one

in America is aware of a passage at the end of his famous tape on November 1, 2004, released right before the election:

> It is easy for us to provoke and bait this administration. All that we have to do is to send two mujahidin [jihadists] to the furthest point east to raise a piece of cloth on which is written al-Qaeda, in order to make the generals race there to cause America to suffer human, economic, and political losses without their achieving for it anything of note other than some benefits for their private companies…
>
> So we are continuing this policy in bleeding America to the point of bankruptcy. …That being said…when one scrutinizes the results, one cannot say that al-Qaeda is the sole factor in achieving those spectacular gains.
>
> Rather, the policy of the White House that demands the opening of war fronts to keep busy their various corporations – whether they be working in the field of arms or oil or reconstruction – has helped al-Qaeda to achieve these enormous results.
>
> And so it has appeared to some analysts and diplomats that the White House and us are playing as one team towards the economic goals of the United States, even if the intentions differ….for example, al-Qaeda spent $500,000 on the event [the 9/11 attacks], while America, in the incident and its aftermath, lost – according to the lowest estimate – more than $500 billion.
>
> Meaning that every dollar of al-Qaeda defeated a million dollars by the permission of Allah, besides the loss of a huge number of jobs.[22]

Know your enemy is the first rule of combat. The War on Terror conceals itself as our enemy by also concealing the true nature of al-Qaeda and its clones. For if we were able to base our policies on the actual capabilities, intentions, weaknesses, and potential strengths of Muslim extremists of the al-Qaeda variety, we would assuredly be able to develop a mode of vigilance and a plan of attack that would be both sustainable and effective. With no theory of our enemy whatsoever, apart from imagining we are faced with an "all azimuth," constant, and utterly ruthless threat of attack from the "Universal Adversary," we find ourselves as if immersed in a pot of water atop a stove. Fearful that neighboring molecules might suddenly burst into steam we expend fruitless efforts scanning every molecule in sight, seeking ways to predict which one will burst into steam next in order to stop it before it does. Obviously, a more sensible strategy is to put our emphasis on turning down the heat under the pot. This strategy calls for political action and diplomacy to engage the Muslim world as a whole on issues of mutual and practical concern, thereby isolating the jihadists from the mass of Muslims whose sympathies our War on Terror has so far helped transform in favor of the jihadists.[23]

This will mean breaking the grip the War on Terror has on our political system and on the debate in America over how to respond to "terrorists with global reach." It means returning, as we did after overcoming the McCarthy-ist hysteria of the early 1950s, to a policy based on realistic assessments of our enemies' intentions, capabilities, and weaknesses, and on confident assessments of our own resilience as a nation. Until we do so, we will cripple our ability to focus

properly on security problems that do exist, and instead remain trapped in the War on Terror.

*Ian S. Lustick is professor of political science at the University of Pennsylvania where he holds the Bess W. Heyman Chair. Professor Lustick is the author of numerous books, including* Trapped in the War on Terror *(2006) and the author of articles on ethnic conflict, Middle East politics, American foreign policy, social science methodology, and organization theory that have appeared in many journals. His current research focuses on aspects of the long-term dynamics of the Israeli-Arab conflict as well as development and applications of agent-based modeling techniques for the solution of problems pertaining to identitarian conflict, political cascades, and political violence. He can be contacted via his website, www.trappedinthewaronterror.com.*

---

[1] Information collected via searches in late October 2005 on the official Department of Defense Web site, http://www.defenselink.mil.

[2] *CBS News/New York Times* Poll. Sept. 15-19, 2006. N=1,131 adults nationwide. MoE ± 3 (for all adults), http://www.pollingreport.com/terror.htm.

[3] For a close analysis of the distance between *24*'s fictionalized world and the actual world of counter-terrorism in America see Spencer Ackerman, "How Real Is '24'?" http://www.salon.com/ent/feature/2005/05/16/24/index.html.

[4] http://www.tv.com/tracking/viewer.html&ref_id=28827&tid=80733&ref_type=101, The show was advertised with the come-on "What do you really know about your neighbors?"

[5] Transactional Records Access Clearinghouse, "Criminal Terrorism Enforcement in the United States During the Five Years Since the 9/11/01 Attacks," Syracuse University, September 4, 2006, http://trac.syr.edu/tracreports/terrorism/169/.

[6] Amy Waldman, "Prophetic Justice," *The Atlantic Monthly* (October 2006), http://www.theatlantic.com/doc/200610/waldman-islam. On the absence of evidence for the presence of a serious terrorist threat inside the United States see especially John Mueller, *Overblown* (New York: Free Press, 2006).

[7] The Oxford English Dictionary defines a cabal as a "small body of persons engaged in secret or private machination or intrigue; a junto, clique, cóterie, party, faction." Secretary of State Powell's chief of staff from 2002 to 2005, Lawrence B. Wilkerson used the term "cabal" to describe the supremacist faction led by Vice President Cheney and Secretary of Defense Rumsfeld against which he, Powell, and other pragmatists fought a losing battle. Lawrence B. Wilkerson, "The White House Cabal," *Los Angeles Times*, October 25, 2005. See also Joshua Muravchik, "The Neoconservative Cabal," *Commentary* 116, no. 2 (September 2003): 26-33. My own first use of the term to describe the neoconservative core of the group driving the country toward war in Iraq was in a Middle East Policy forum on Capitol Hill on October 1, 2002. See http://www.campus-watch.org/article/id/442, and http://www.mepc.org/public_asp/forums_chcs/31.asp.

[8] Other prominent neoconservatives associated with the *Weekly Standard* include executive editor Fred Barnes along with Charles Krauthammer, Reuel Marc Gerecht, and David Frum, all listed by the magazine as contributing editors.

[9] William Kristol and Robert Kagan, "Toward a Neo-Reaganite Foreign Policy," *Foreign Affairs* 75, no. 4 (July/August 1996): 18-32.

[10] http://www.newamericancentury.org/iraqclintonletter.htm, For sympathetic treatments of the meaning of "neoconservative," see Mark Gerson, *The Neoconservative Vision: From the Cold War to the Culture Wars* (Lanham, Md.: Madison Books: 1996); Muravchik, "Neoconservative Cabal." For a very different view see Anne Norton, *Leo Strauss and the Politics of American*

*Empire* (New Haven, Conn.: Yale University Press, 2004). For the backgrounds of some key neoconservative activists see George Packer, *The Assassins' Gate* (New York: Farrar, Straus and Giroux, 2005), 15-32. For Armitage's "defection" to the Powell camp that tried to block the PNAC agenda, he was widely regarded within the cabal as a political traitor.

[11] Regarding the decisiveness of inside-the-beltway brawls between the pragmatic and supremacist wings of the first George W. Bush administration see Ian S. Lustick, *Trapped in the War on Terror* (Philadelphia: University of Pennsylvania Press, 2006), 48-70.

[12] For details on the complex and confusing history of these lists see Office of Inspection and Special Reviews, Office of the Inspector General, Department of Homeland Security, *Progress in Developing the National Asset Database*, OIG_06_40 (June 2006) and John Moteff, *Critical Infrastructure: The National Asset Database*, Resources, Science, and Industry Division, Congressional Research Service (September 14, 2006).

[13] Steve Friess, "NRA Counts on 9/11 Momentum at Convention," *USA Today*, April 25, 2002. For an insightful study of how the larger movement of gun rights activists have changed their narrative to capitalize on the War on Terror, see Christy Allen, "The Second Amendment IS Homeland Security: American Gun Rights Activism Post September 11, 2001," http://www.essex.ac.uk/sociology/postgraduates/6_allen.pdf.

[14] Ibid., 9.

[15] Loren Berger and Dennis Henigan, "Guns and Terror: How Terrorists Exploit Our Weak Gun Laws," Brady Center to Prevent Gun Violence, 2001, http://www.bradycenter.org/xshare/pdf/reports/gunsandterror.pdf.

[16] *Journal of Veterinary Medical Education* 30, no. 2 (2003), http://www.utpjournals.com/jvme-feature-article.html.

[17] U.S. Senate Committee on Appropriations, Subcommittee on Labor, Health and Human Services, and Education statement, on behalf of the American Academy of Pediatrics, Senate, 107th Cong., Second Sess., April 15, 2002, 1, 5-6.

[18] For a letter to Congress signed by eleven professional and trade associations linked to the pharmaceutical industry and listing this and other recommended measures see the Web site of the Academy of Managed Care Pharmacy at http://www.amcp.org/data/legislative/analysis/21202.pdf.

[19] For one such initiative based at the University of Pennsylvania, where I teach, see the Institute for Threat Analysis and Response (ISTAR), where I myself am listed as a resource person, http://www.istar.upenn.edu/scholars/index.html.

[20] For details and a plethora of examples of the dynamics of the "War on Terror whirlwind" see Lustick, *Trapped in the War on Terror,* 71-114.

[21] The executive summary of the National Planning Scenarios study explains the term "Universal Adversary" as follows: "Because the attacks could be caused by foreign terrorists; domestic radical groups; state-sponsored adversaries; or in some cases, disgruntled employees, the perpetrator has been named, the Universal Adversary (UA)." The authors of the study justify this abstraction by stressing that the "focus of the scenarios is on response capabilities and needs, not threat-based prevention activities." What is instructive is the attempt to separate "responses" from threats. What could be more reinforcing for an ever-expanding War on Terror than imperatives to prepare for dangers of any kind, whether threats are perceived to exist or not, simply because when dealing with the "Universal Adversary," anything is possible? David Howe, senior director for response and planning, *Planning Scenarios: Executive Summaries,* The Homeland Security Council, July 2004, http://cryptome.org/15-attacks.htm.

[22] For the full transcript of bin Laden's speech, broadcast on Al-Jazeerah on November 1, 2004, see http://english.aljazeera.net/NR/exeres/79C6AF22-98FB-4A1C-B21F-2BC36E87F61F.htm.

[23] For a discussion of American options in this regard see Ian S. Lustick, *Trapped in the War on Terror*, 140-145.

# Expecting the Unexpected: The Need for a Networked Terrorism and Disaster Response Strategy

W. David Stephenson and Eric Bonabeau

## INTRODUCTION

Hurricane Katrina focused attention on improving the command-and-control management response to natural disasters and terrorist attacks. But what if the command-and-control approach itself is so fundamentally mismatched to dealing with unpredictable, rapidly-changing circumstances (including the incapacitation of command personnel and technology), commonplace in natural disasters or terrorist attacks, that, even if improved, it is still unequal to the task?

The emphasis placed on improving command and control should instead be focused on creating a new, alternative emergency management approach capitalizing on a combination of new communications technology and the science of social networks and "swarm intelligence" that is fundamentally better matched to the circumstances encountered in disasters. The hallmarks of such a strategy would be flexibility, ease of incorporating situational awareness into decision-making, and the ability of anyone available after a catastrophe to create *ad hoc* strategies with available resources.

### Katrina's Lessons

All the major analyses of the failures in preparing for and responding to Hurricane Katrina highlighted management failures at all levels of government.[1] Perhaps most succinct was the House Select Committee's report:

> [D]uring and immediately after Hurricane Katrina made landfall, there were lapses in command and control within each level of government, and between the three levels of government…. The lack of effective command and control, and its impact on unity of command, degraded the relief efforts. [2]

The Department of Homeland Security (DHS) was established and the Federal Emergency Management Agency (FEMA) was put under its aegis in part to improve coordination and delivery of services after a natural disaster or terrorist attack. However, the utter chaos after Hurricane Katrina, both in management and delivery of services, demonstrated the flaws in the secretariat's structure and strategy: DHS overall, and FEMA in particular, was inflexible, lacked redundancy, was slow to react to changing conditions, and – when the ordinary chain of command was interrupted – individual components were not able to adapt and become self-directed. In New Orleans, vital supplies and personnel did not arrive until three days after the hurricane made landfall.[3]

While most recommendations in the four major analyses of Katrina focused on how to strengthen traditional command-and-control management, this essay concentrates instead on how to plan for the all-too-likely situations following a disaster or terrorist attack (such as Katrina or the World Trade Center on 9/11) when circumstances arise that could not be visualized in advance, and responders are themselves victims or their ordinary command structure is compromised. In these situations, whoever survives and

is available must cobble together *ad hoc* solutions in response to rapidly-evolving situations.

## ALTERNATIVE MODEL: NETWARS

A model for an effective alternative to command-and-control in disasters or terrorist attacks is found in a 1996 study for the Defense Department, *The Advent of Netwar*.[4] In it, John Arquilla and David Ronfeldt describe the rise of networked enemies "[who are] organized along networked lines or employ networks for operational control and other communications."[5] They claim the information revolution encourages this shift.

Arquilla and Ronfeldt argue this new type of enemy requires rethinking U.S. defense strategy because it gives small groups who communicate, coordinate, and conduct their campaigns in a networked manner, without a precise central command, an advantage over hierarchical opponents.[6] Logically, fighting a networked enemy requires the U.S. to form networks to fight networks, decentralizing operational decision-making authority.

In recent years the Department of Defense has begun to develop and deploy such strategies under names such as network-centric warfare or "power to the edge" (although the approach is by no means universally accepted).

This essay examines the possibility of extending the networked concept to respond to domestic terror attacks or natural disasters. Since domestic terror cells are likely to employ the same kind of loosely-knit networks as their Middle Eastern counterparts, the "netwar" approach would seem directly relevant when responding to a terrorist attack at home.

At the same time, natural disasters whose effects cannot be predicted accurately from past occurrences, which involve rapidly-changing circumstances, and which exact their greatest toll on the most vulnerable, might be seen as the natural world's analog to terrorist networks, making a flexible, networked strategy also relevant to natural disaster response.

### Networked Communication and Science of "Swarm Intelligence" Combine

A combination of two factors – one technological and the other scientific – have emerged during the past twenty years, presenting the potential for a strategy that would not only facilitate flexible disaster and terrorism response, but could actually foster creative, *ad hoc* solutions to unforeseen situations that emerge during a crisis.

The first of these factors is the growing body of scientific understanding of "swarm intelligence" or "emergent behavior." This discipline began with empirical observation of the behavior of social insects such as bees, ants, and termites. Social insects have meager intelligence yet, through collaborative, self-organizing action, create highly-sophisticated structures and collaborative projects. Researchers have created rigorous mathematical formulas to describe the activities of social insects, and are now applying those formulas to human management issues.[7]

The second factor is the development and widespread adoption of networked communications technologies and applications. This includes text messaging and self-organizing, self-healing "mesh" wireless computer networks, which can continue to function when conventional communications infrastructure is damaged and destroyed, and which can be controlled directly by end users without the need for, or control by, central authorities.

## Applicability of Swarm Intelligence to Terrorism and Disaster Response

Three characteristics of "swarm intelligence" particularly relevant to emergency management are flexibility, robustness, and self-organization.[8] Most people would agree that all three of those characteristics were missing from the governmental response to Katrina.

The single noteworthy agency exempted from the criticism of governmental response was the U.S. Coast Guard, whose Gulf Coast units did not wait for express authorization to begin search and rescue operations. According to a Government Accountability Office report, "… underpinning these efforts were factors such as the [Coast Guard's] operational principles. These principles promote leadership, accountability, and enable personnel to take responsibility and action, based on relevant authorities and guidance."[9]

Similarly, on 9/11 the only effective response was a classic example of swarm intelligence. A group of total strangers on Flight 93 coalesced (in circumstances when no one would have blamed them for instead dissolving into hysterics) to thwart the hijackers' plan to crash the plane into the Capitol or White House. They exhibited all three characteristics of swarm intelligence in abundance.

Another example is how individuals came together via the Internet to provide a variety of invaluable and reliable information to victims of the tsunami, and, more recently, of Hurricane Katrina. In particular, some of these people took it upon themselves to create the *tsunamihelp* blog and wiki[10]. Later, a core group of those people took the lead in creating the *Katrinahelp* wiki. As one of the *tsunamihelp* volunteers, Dina Mehta, wrote:

> We experienced a near-magical interdependence as we were setting up and establishing this blog. It's not just about the people who were blogging; there [were] a whole lot of volunteers who fed us with links, sent us letters from affected people reaching out for help, others who took on the mantle of editing, sub-groups working on design and template issues, still others quietly contributing by buying up bandwidth and applications and offering up mirror servers, that made the blog more effective. [11]

Mehta accurately describes how individuals participating in a situation that evokes swarm intelligence produce results that are far greater than the sum of their parts. In the case of Katrina, still others spontaneously came together to craft imaginative Google Map mashups (applications combining information from multiple sources) to allow identification of homes in New Orleans[12] and to create unified databases of those needing assistance.[13]

Perhaps the most astonishing examples of swarm intelligence in a recent disaster response situation were the variety of *ad hoc* rescue efforts in New Orleans that Douglas Brinkley described in *The Great Deluge*. Spurred by word of mouth, hundreds of Cajuns spontaneously navigated their small boats to New Orleans in an *ad hoc* citizens' flotilla, the "Cajun Navy," which rescued nearly 4,000 survivors.[14] Reggae singer Michael Knight and his wife Deonne saved approximately 250 people by themselves.[15] Richard Zuschlag, co-founder of Acadian Ambulance Service, used his 200 ambulances, plus medivac helicopters, to evacuate 7,000, while also providing the only reliable emergency communications system.[16]

## Networked Personal Communication Devices Foster Swarm Intelligence

These examples demonstrate that swarm intelligence is possible even under the trying circumstances of a terrorist attack or a natural disaster. But does this warrant encouraging swarm intelligence as a formal part of homeland security planning, and, if so, how can it be done?

In part, fostering emergence should be part of the plan because networked personal communications technology has, in effect, already made the choice for us, whether or not officials officially recognize that reality. Just as earlier civilizations used signal fires or semaphores in a disaster, the advances in networked communications, combined with human nature, make it almost inevitable that individuals during a disaster will automatically turn to the increasing array of electronics they use every day to reach out to others for comfort and mutual assistance.

Equally important but less understood by decision makers, and unlike landline phones or the broadcast media, these new communication devices are themselves increasingly networked, and those networks are self-organizing, and self-healing. In many cases (such as mesh networks that were originally developed for the military in battlefield conditions and now are being used by civilians) the networks do not require any kind of external networking. By simply turning on two or more devices equipped with mesh network cards (or free software from the CUWiN project),[17]the network self-organizes.

(It is noteworthy that the One Laptop Per Child project, which aims to distribute millions of laptops costing $100 each to impoverished schoolchildren worldwide, believes the ability to create instant networks is so important that it includes a built-in mesh capability in each computer.[18] Equally important, if one or more nodes are disabled, the network can still function; it simply routes around the interruption.)

Even cell phones still functioned during both 9/11 in Manhattan and in New Orleans during Katrina, for those who knew how to use them correctly under the circumstances. Although voice mails would not go through, packet- and IP-based SMS text messages did, because they use minimal bandwidth and can route around obstacles.[19]

Authorities may have little choice in factoring these communication devices into emergency communication strategies because so many are controlled by end users who will use them in a disaster. Used inappropriately and without guidance, these devices could consume all available bandwidth and crash networks. By contrast, if officials provide guidance before a disaster on how to use networked communications appropriately, those communication devices could be an important expansion of the new phenomenon of "sousveillance" (i.e., the opposite of surveillance). Sousveillance is frequently associated with using camera phones or video cameras to document official malfeasance.[20] In disasters or after terrorist attacks, it could also refer to individuals using those devices not only to spread information among survivors, but actually to provide information about damage, those in need of assistance, etc. that could be incorporated into the situational awareness network. If disaster processes were revamped on the basis of systems dynamics to include built-in feedback loops, this information could be fed into the system for rapid correction.

It is one thing for individuals to have communication devices they can use for mutual benefit during a crisis. Having a large number of individuals – in close physical or virtual proximity – merely coexisting does not assure swarm intelligence. For swarm intelligence to emerge, they must interact.

### Wikis and Other Web 2.0 Collaborative Tools

A second related technological development could foster this necessary interaction. These are so-called collaborative software programs, particularly wikis, which are designed specifically to allow participation by a wide range of people on a self-organizing basis. These are frequently referred to as Web 2.0 applications, for which the Web itself is the platform (a critical consideration in a crisis, since the Web does not reside on a single computer that might be unavailable) and which tend to foster collaboration and "harvest collective intelligence."[21]

As has been widely reported,[22] almost any wiki, at any point in time, will contain erroneous information. However, so do the FEMA and DHS websites. The difference is that other users can and will quickly correct these errors – much more rapidly than would happen with an official website. As a result, to this day, the *Katrinahelp* wiki remains the single most comprehensive and authoritative source of information for survivors. Similarly, a recent study demonstrated that the all-volunteer written *Wikipedia* is as, if not more, accurate than the peer-reviewed *Encyclopedia Britannica*.[23] A recent report by the highly-respected Center for Strategic and International Studies, "Wikis, Webs, and Networks: Creating Connections for Conflict-Prone Settings," recommending that governments and NGOs consider using wikis and other social networking applications to deal with what they term "collapsed and fragile states" globally, concluded that "... in many cases, the daily benefits of open information systems [such as wikis] outweigh the potential threats."[24]

*Katrinahelp* is also a prime example of swarm intelligence. Working in isolation from each other the contributors could never have created its rich content; it was precisely the give-and-take of the collaborative editing process that *made Katrinahelp* so informative.

## BASIC STRUCTURE OF A NETWORKED DISASTER AND TERRORISM RESPONSE

We cannot detail the structure of such a networked homeland security system in a paper of this length. However, the basic structure of such a system includes:

- An opt-in system that would allow willing members of the public to become part of the network, both providing and receiving information while preserving non-participants' privacy.
- Legal and technological barriers to capricious use of the system to avoid having it used as a tool for discrimination or petty harassment.
- Coordination of all the components through new "presence" applications that allow creation of instant networks and sharing of real-time, location-based information.[25]
- An effort to involve a variety of commercial applications that are familiar to the general public (so there will be no learning curve if they are used in a crisis, unlike dedicated governmental emergency communications systems that are unfamiliar to the public and must be learned in the midst of a crisis), particularly ones that serve to create online and physical social networks, thereby fostering "swarm intelligence."

## Portland Connect and Protect Program Shows Network Approach Works

One system already in operation will illustrate how networked communications devices, combined with the applications private-sector entrepreneurs create and refine constantly to exploit these devices' power (especially applications providing location-based, real-time information that would be critical in a disaster), foster swarm intelligence in emergencies.

Swan Island Networks, the non-profit Regional Alliances for Infrastructure and Network Security (RAINS), and the City of Portland transformed the city's 911 system to make it truly interactive.[26] The system analyzes and synthesizes incoming warnings, then redistributes them not only to EMTs and police, but also to hospitals, schools and other institutions, as well as to willing members of the general public.

While not part of the original design, participants now communicate with each other as well with central authorities. For example, parole officers send alerts to the school, and hotel managers pass along storm threats (often more rapidly than the official warnings).

> Connect & Protect is now a large conglomeration of overlapping alerts stretching across nine Oregon counties. Each stream of warnings is controlled by the agency that issues it. Fairly strict security features attempt to limit abuse of the warnings – certain categories of calls, such as reports of sexual crimes, are not transmitted publicly, the alerts can't easily be copied or pasted, anonymity is forbidden.[27]

A *Wired* magazine article about the Connect and Protect program concluded with a paragraph summarizing this essay's contention as well. A comprehensive terrorism and natural disaster response strategy must include a fall-back approach in the likely situation that circumstances are unprecedented and/or first responders are overwhelmed:

> If national safety – the ability to respond to hurricanes, terrorist attacks, earthquakes – depends on the execution of explicit plans, on soldierly obedience, and on showy security drills, then a decentralized security scheme is useless. But if it depends on improvised reactions to unknown threats, that's a different story. A deeply textured, unmapped system is hard to bring down. A system that encourages improvisation is quick to recover. Ubiquitous networks of warning may constitute our own asymmetrical advantage, and, like the terrorist networks that occasionally carry out spectacular attacks, their power remains obscure until they're called into action.[28]

As Portland's Connect and Protect demonstrates, a networked homeland security strategy is feasible today, using existing technology and requiring much less time to create and deploy than some of the costly, dedicated emergency communications systems government is creating. Equally important, by facilitating those three qualities of swarm intelligence needed in a crisis (flexibility, robustness, and self-organization), such a strategy could transform the general public from hopeless victims, waiting for aid that may never come, into self-reliant components of the overall response, able to craft *ad hoc* strategies to respond to fast-changing circumstances.

## CONCLUSION

So why is a networked homeland security strategy not under consideration? While

executives can relate easily to the flexibility and robustness aspects of swarm intelligence, they may find it harder to deal with the concept of self-organization, probably because that carries with it a loss of their ability to exercise top-down command-and-control.

However, as mentioned earlier, a technological imperative is at work. Due to the potential of networked personal communications devices to function in a crisis, independent of (or despite) a central authority, officials really do not have a choice in embracing a networked disaster and terrorism response strategy. Government has already effectively lost control of the flow of information during emergencies. The public now has the power at their fingertips to network in a disaster – and human nature dictates that they will use it.

Polls have shown that, since Katrina, the public has lost faith in government's ability to protect them.[29] Those same polls show that individuals are taking more steps to prepare to help themselves in a disaster.[30] Government can capitalize on the technology and science of networks and treat the public as full partners in prevention and response, creating the conditions that would directly foster swarm intelligence, or the people may simply take matters into their own hands and circumvent the government during natural disasters and terrorist attacks.

*W. David Stephenson is principal, Stephenson Strategies (Medfield, MA). A former corporate crisis and Internet consultant, he specializes in homeland security strategies to empower the general public. He writes a blog on homeland security and is a frequent speaker at conferences.*

*Eric Bonabeau is chief executive officer and chief scientific officer of Icosystem, (Cambridge, MA) which uses the tools of complexity science and advanced computational techniques to provide software simulation tools for exploring business issues and strategies. He is one of the world's leading experts in complex systems and distributed adaptive problem solving, and spent several years as a research fellow at the Santa Fe Institute. Bonabeau is co-editor-in-chief of the* Advances in Complex Systems*, and co-author of* Intelligence Collective, Swarm Intelligence, and Self-Organization in Biological Systems.

---

[1] The major reports analyzing problems in responding to Katrina include: U.S. House of Representatives, Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative: The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina* (U.S. House of Representatives, 2006); Senate Committee on Homeland Security and Government Affairs, *Hurricane Katrina: a Nation Still Unprepared*, (U.S. Senate, 2006); Frances F. Townsend, *The Federal Response to Hurricane Katrina: Lessons Learned* (White House, 2006); Office of Inspector General, Department of Homeland Security, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina*" (Department of Homeland Security, 2006).

[2] U.S. House of Representatives, *A Failure of Initiative*, 186.

[3] Douglas Brinkley, *The Great Deluge* (New York: Morrow, 2006), 245-51, 635.

[4] John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica: Rand, 1996).

[5] Ibid., 1.

[6] Ibid., 82.

[7] Derek Story, "Swarm intelligence: an interview with Eric Bonabeau," *P2P.com*, 2003, http://www.openp2p.com/pub/a/p2p/2003/02/21/bonabeau.html. "With self-organization, the behavior of the group is often unpredictable, emerging from the collective interactions of all of the individuals. The simple rules by which individuals interact can generate complex group behavior. Indeed, the emergence of such collective behavior out of simple rules is one the great lessons of swarm intelligence. "

[8] Eric Bonabeau and Christopher Meyer, "Swarm Intelligence: a whole new way to think about Business," *Harvard Business Review* (May 2001): 108.

[9] Government Accountability Office, "Coast Guard: Observations on the Preparation, Response, and Recovery Missions Related to Hurricane Katrina," GAO-06-903, (2006), http://www.gao.gov/new.items/d06903.pdf.

[10] *Katrinablog*, http://www.katrinablog.org/; *Katrinahelp* wiki, http://katrinahelp.info/wiki/index.php/MainPage.

[11] Dina Meta, "Social Tools - Ripples to Waves of the Future," *Global Knowledge Review* (2005), http://www.gurteen.com/gurteen/gurteen.nsf/id/gkr2005-05.

[12] David M. Ewalt, "Google is Everywhere," *Forbes.com*, September 2, 2005, http://www.forbes.com/technology/2005/09/02/hurricane-google-map-rescue-cx_de_0902google.html.

[13] W. David Stephenson, "Katrina Data Project & Public Web Stations: smart mobs in action," W. David Stephenson blogs on homeland security et al., September 27, 2005, http://stephensonstrategies.com/2005/09/27.html.

[14] Brinkley, *The Great Deluge*, 381.

[15] Ibid., 306.

[16] Ibid., 458.

[17] W. David Stephenson, "CUWiN already visualized low-cost mesh net for emergency use," *W. David Stephenson Blogs on Homeland Security et al.*, http://stephensonstrategies.com/2005/08/31.html#a450.

[18] One Laptop Per Child, http://www.laptop.org/faq.en_US.html.

[19] Jennifer McAdams, "SMS does SOS," *Federal Computer Week*, April 3, 2006, http://www.fcw.com/article92790-04-03-06-Print.

[20] Wearcam.org, "Secrecy, not privacy, may be the true cause of terrorism," http://wearcam.org/sousveillance.htm.

[21]Tim O'Reilly, "What is Web 2.0," *O'Reilly.com*, September 30, 2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

[22] Jim Giles, "Internet Encyclopedias Go Head to Head," *Nature.com*, December 14, 2005, http://www.nature.com/news/2005/051212/full/438900a.html.

[23]Stacy Schiff, "Know It All," *The New Yorker*, Aug. 31, 2006, http://www.newyorker.com/fact/content/articles/060731fa_fact.

[24] Rebecca Linder, "Wikis, Webs, and Networks: Creating Connections for Conflict-Prone Settings" (Washington: Council for Strategic and International Studies, 2006), http://www.csis.org/component/option,com_csis_pubs/task,view/id,3542/type,1/.

[25] W. David Stephenson, "Roaming Presence: hot presence application for emergency use," *W. David Stephenson Blogs on Homeland Security et al.*, http://www.stephensonstrategies.com/2005/10/24.html#a576.

[26] Gary Wolf, "Reinventing 911," *Wired*, December 2005, http://www.wired.com/wired/archive/13.12/warning.html.

[27] Ibid.

[28] Ibid.

[29]ABC News, "Poll: Confidence in Anti-terror response Drops," October 9, 2005, http://abcnews.go.com/Politics/PollVault/story?id=1189755&page=1.

[30]Ibid.

# Deterrence, Terrorism, and American Values

Uri Fisher

## INTRODUCTION

In the aftermath of the September 11 attacks on the World Trade Center and the Pentagon, academics and policymakers were quick to dismiss the strategic role that deterrence could play in U.S. counterterrorism policy. President George Bush's often quoted conclusion that traditional concepts of deterrence are meaningless against "shadowy terrorist networks" with no nation to defend and who are willing to engage in "wanton destruction" resonated throughout discussions on U.S. national security strategy. A 2002 RAND report asserted, "Deterrence is both too limiting and too naïve to be applicable to the war on terrorism."[1] Since September 11, deterrent strategies have repeatedly been characterized as relics of the Cold War era of superpower confrontation. As a result, the White House has focused on defensive and preemptive counterterrorism strategies. The current administration argues that the U.S. can no longer wait for the worst security threats, such as terrorists acquiring chemical, biological, radiological, and nuclear weapons (CBRN), to materialize before acting.

Alternatively, many commentators and researchers, especially in the field of political science, maintain that deterrence remains a viable and utilizable tool in U.S. policymakers' arsenal to combat terrorism. Regardless of which side of the fence analysis falls on this issue, however, an important aspect of the deterring terrorism argument receives very little attention – the role that ideals and values play in America's ability to establish a deterrent mechanism against terrorists. I argue that deterrence, as a strategic concept, is not inapplicable to defending against terrorism; however, the U.S. would face considerable legal and moral quandaries if it were to carry out the necessary policies to deter terrorists and their supporters. To be sure, some elements of a terrorist organization can be deterred, but it is unlikely that U.S. policymakers are willing to sacrifice core American values in order to credibly signal to these actors that something "they hold dear" is in jeopardy if they commit or support terrorist aggression. To establish a deterrent mechanism against terrorist networks the U.S. would be required to explore a number of extremely heavy-handed policy options, such as regime change, nuclear retaliations, and expanding targeted killing operations to included terrorists' family members and loved ones.

Implementing policies such as these are the only ways to effectively deter elements of a terrorist organization and its support structure. Nevertheless, doing so would force the U.S. to take certain positions that would come into conflict with American ideals and beliefs about justice, fairness, and human rights. Moreover, policy pronouncements that could deter terrorists would be inflammatory and would most likely be met with considerable domestic and international criticism. Even when the U.S. has "skirted" some of these policies in recent years to combat terrorism, controversy and disagreement have emerged over the morality and legality of such actions.

The simplistic argument that terrorists cannot be deterred is reductionist. Additionally, those who argue that deterrence maintains significant utility in the U.S.

war on terror fail to acknowledge the level of harshness and brutality required of U.S. policy to establish a deterrent mechanism against members of terrorist networks. What really prevents the U.S. from deterring terrorists is not the simple unsuitability of the strategic concept of deterrence, but America's humanity, civility, and idealism.

## DETERRENCE AND TERRORISM

By now, the arguments are familiar for why deterring a group such as al-Qaeda is a complex endeavor. First, terrorists are highly motivated and therefore they are willing to risk anything – their lives in the case of suicide-bombers – to accomplish a goal. Second, the political goals of terrorist groups are often very broad, idealistic, ambiguous, or unclear. Third, terrorists are difficult to locate. Terrorist networks operate trans-nationally and therefore make reprisals difficult to "return to sender." Fourth, it remains undecided how deterrence can work against an enemy that understands that the ultimate policy goal of the U.S. is not to coexist with groups like al-Qaeda, but to eradicate them. Finally, terrorists often attempt to incite retaliation. Terrorists have used the collateral damage caused by retaliatory efforts to foment more support for their organization or broader cause. In total, the deck is stacked against deterrence playing a significant role in U.S. counterterrorism policy.

While most post-September 11 analyses conclude that deterrence is of little use against terrorists, some maintain that the "death of deterrence" has been exaggerated and that deterrence can remain a key component in the war on terror.[2] One rationale for the argument that deterrence is not "dead" is that September 11 did not illustrate the irrelevance of deterrence, but rather that U.S. foreign policy throughout the 1980s and 1990s had failed to communicate to al-Qaeda that the U.S. was willing and able to inflict significant suffering on terrorist transgressors. That is, deterrence did not fail; rather the U.S. had failed to establish an effective deterrent mechanism against al-Qaeda. As President Bush noted in 2001, "It was clear that bin Laden felt emboldened, and didn't feel threatened by the United States."[3]

The list of instances in which the U.S. was attacked by Islamic radicals but failed to retaliate in any meaningful manner is well known: Tehran in 1979, Beirut in 1983, the World Trade Center in 1993, the Khobar Towers in 1996, the U.S. embassies in East Africa in 1998, and the USS Cole in 2000. All of these cases evoked principled lectures and saber-rattling by U.S. presidents on how the U.S. must fight terrorism, yet rarely were these strong proclamations accompanied by actual deeds. Furthermore, the events that unfolded in Somalia in 1993 signaled to U.S. enemies that the U.S. was unwilling to suffer costs in blood to realize its policy goals. Some even argue the U.S. continues to be afflicted by a "Vietnam syndrome." This reticence to retaliate and aversion to casualties did not go unnoticed by al-Qaeda's leadership. Osama bin Laden repeatedly painted the U.S. as a "paper tiger," a country more apt to growl than bite.

The second argument made for the continued applicability of deterrence is that terrorist networks are hierarchical organizational structures. Terrorist organizations are comprised of many actors, each with different responsibilities, roles, and motivations. The fanatical individuals who carry out suicide bombings or other types of attacks represent only a small portion of a terrorist organization. Many other actors, such as financiers, recruiters, leaders, religious figures, and state supporters are also important components of a terrorist organization. These different elements have come to be known

as the "al-Qaeda system." It is suggested that while the "foot soldier" who is willing to blow him/herself up in a crowded marketplace is probably undeterrable, deterrence may be possible against other entities that comprise a terrorist network. Some actors within a terrorist network may have a clearer cost-benefit conceptualization, possess assets that are more easily targeted, or are simply less motivated than other elements within the organization.

Although terrorist networks should be understood as complex organizations, the dilemma of effectively deterring the actors who comprise a terrorist system remains. First, security strategists must distinguish what these diverse actors actually value. Second, defense planners must establish a *meaningful* threat of punishment in the event of a terrorist attack against the U.S. or its interests. As Thomas Schelling noted, "To exploit a capacity for hurting and inflicting damage one needs to know what an adversary treasures and what scares him."[4] The U.S. must be able to credibly communicate and signal to the different actors in a terrorist network that what they value will be put at risk. Bombing baby formula factories in the Sudan and empty tents in Afghanistan, as the U.S. did in response to the 1998 embassy bombings in Africa, does not constitute damaging what terrorist elements hold dear. Establishing a deterrent mechanism requires not just any retaliation, but focused and consequential retaliation.

Recent comments by French President Jacques Chirac and Colorado Congressman Tom Tancredo intensified the debate over how retaliatory threats are communicated to terrorists. President Chirac, speaking at a submarine base in Brittany in January 2006, stated that France was prepared to carry out a nuclear strike against any country that sponsors a terrorist attack against French interests. Chirac went on to say that France's nuclear arsenal is now organized to include the ability to retaliate against a terrorist attack with tactical nuclear strikes.[5] President Chirac was clearly sending a warning to Iran and various Arab countries that continue to support terrorist organizations. In a more reckless assertion, Congressman Tom Tancredo stated in 2005 on a Florida radio talk show that the U.S. could consider "taking out" Muslim holy sites if terrorists attacked the U.S. with nuclear devices. Both comments created a public storm, as many observers quickly labeled these statements irresponsible.

Notwithstanding the merit or lack thereof of such comments, the response that these statements engendered revealed another problem with the possibility of establishing a deterrent mechanism against terrorists. Because effective deterrence requires the U.S. to directly threaten targets of value to terrorist elements, a dilemma arises: whether the U.S. would be willing to carry out the necessary actions to credibly communicate to terrorist elements that what they value is at risk if terrorist acts occur. What targets must the U.S. threaten for a potential terrorist element to estimate that the costs of carrying out a course of action are unacceptably high? Is the U.S. prepared to implement policies that may evoke strong dissent from certain segments of the domestic and international community? Can the U.S. credibly threaten these targets without crossing certain ethical, political, and legal boundaries of behavior?

U.S. foreign policy has always been a manifestation and extension of the basic values, principles, and beliefs on which the American republic was founded.[6] In dealing with terrorists, the U.S. has sought rational, reasoned, and relatively proportional responses in order to maintain the respect of the international community and its own citizens. However, to deter certain terrorist elements the U.S. will ultimately find it necessary to

compromise certain democratic values that have long guided its foreign policymaking. Because the U.S. cares about projecting an image of virtue, it is unlikely that it will ever truly be able to put at risk what terrorist elements value. The current war on terrorism has already revealed the inherent conflict between maintaining a foreign policy that reflects the reality of U.S. capabilities while remaining dedicated to democratic ideals. As Clifford Kupchan has argued, Americans want both a muscular and moral foreign policy.[7]

Unfortunately, measures that may prove functional in establishing a deterrent mechanism against a group like al-Qaeda may not be viable in light of the core values of the country, even in a time of war. The politically incorrect promise of violent retaliation following a terrorist attack is the only significant course of action when attempting to establish a deterrent mechanism against members of the al-Qaeda system.[8] Those who argue that deterrence is still relevant in dealing with terrorism fail to consider the actual policies the U.S. will have to pursue in order to deter terrorists from carrying out violent acts.

Most examinations of deterrence and U.S. counterterrorism policy make the common argument that the U.S. will have to communicate a clear message of punishment against terrorist elements, without actually considering toward whom and where these threats should be directed. Moreover, in those instances where authors consider targets of retaliation, potential threats of punishment rarely strike at what terrorists truly hold dear. Frequently, policy recommendations represent little more than establishing obstacles to terrorist networks, not meaningful attempts to change the decision-calculus of terrorist elements. The targets the U.S. will be forced to retaliate against and the manner in which these targets will have to be engaged may render the moral price of establishing a real deterrent mechanism too high. Deterrence is impossible against terrorists, not because it is theoretically inapplicable, but because the U.S. is too concerned with maintaining its moral authority in the world. The aspiration of the U.S. to take the "moral high road" will signal to terrorists that the things they value most are actually not in grave danger. When attempting to deter terrorists the "ethical and necessary" ultimately will collide.

## Deterring State Supporters

Deterring state sponsors of international terrorist organizations presents perhaps the most theoretically straightforward attempt to utilize deterrent strategies in the war on terrorism. Even those who are generally skeptical of deterrence being applied to terrorism believe the U.S. may be able to deter states from harboring or supporting terrorist organizations. Of the many elements that comprise a terrorist network, rogue regimes that support terrorists are the easiest to find. Assets of a rogue regime that can be targeted, such as the territory under its control or the lives of the ruling elite, are more apparent than the assets held by individual members of terrorist organizations. Efforts to dissuade states from forming relationships with terrorists also represent one of the critical aspects of the war on terrorism. Indeed, only days after the September 11 attacks, President Bush articulated what came to be known as the Bush Doctrine: "Any nation that continues to harbor or support terrorism will be regarded by the United States as a hostile regime."[9]

The most salient concern for U.S. defense planners is the prospect of rogue states providing CBRN to a group such as al-Qaeda. The U.S. currently lists six countries as

potential state sponsors of terrorism: Iran, Syria, North Korea, Cuba, and Sudan. In 2006 the U.S. State Department removed Libya because it apparently was assisting the U.S. in its war on terror. It appears that over the past few years, state sponsorship of terrorist organizations has waned. Libya, for example, has been cooperating with the U.S. to find Libyan members of al-Qaeda. Even more noteworthy, in December 2003, Colonel Muammar Qaddafi stated that the Libyan government would cease research and development of CBRN and would allow weapons inspectors to confirm its disarmamanent efforts. While the impetus for such positive steps are multifaceted, the U.S. success in ousting the Taliban from power and killing many of its members in Afghanistan has "served notice" to rogue regimes around the world that the U.S. is willing and able to destroy what rogue regimes value. Moreover, the possibility of Saddam Hussein acquiring CBRN and then passing these capabilities along to terrorists was a significant rationale for the U.S. invasion of Iraq. Many argue that Libya's decision to dismantle its CBRN programs and other governments' decisions to ratchet up the pressure they exert on al-Qaeda cells within their borders is at least partly due to a growing fear that U.S. military force might be used against regimes that continue to harbor terrorist organizations.[10] As Vice President Dick Cheney stated in the 2004 vice presidential debate with John Edwards, the Libyan decision to abandon its CBRN programs was one of the "great by-products" of U.S. actions in Iraq and Afghanistan.[11]

While it appears that U.S. military operations and legal actions since September 11 have established a deterrent mechanism against state sponsorship of terrorism, the threat of these initiatives remains a critical concern to policymakers. Osama bin Laden has voiced an interest in acquiring mass-casualty weapons and many analysts suggest that al-Qaeda would not hesitate to use CBRN weapons if it acquired these capabilities. To do so, however, terrorist groups need help, either by smuggling CBRN materials from poorly secured facilities or by developing relationships with foreign governments willing to transfer CBRN capabilities. Thus far, it appears that al-Qaeda's pursuit of CBRN capabilities has been unsuccessful. In 2002, *The New York Times* reported that U.S. administration officials stated that "...analysis of suspected radioactive substances seized in Afghanistan has found nothing to prove that Osama bin Laden reached his decade-long goal of acquiring nuclear materials for a bomb."[12] However, U.S. intelligence agencies suspect that Pakistani scientists gave al-Qaeda members information on how to construct a radiological weapon, or "dirty bomb."[13] North Korea increased the fear of a state transferring weapons materials, when in 2003 it threatened to sell a quantity of plutonium to the highest bidder. Additionally, as Iran is on the cusp of developing nuclear capabilities, this scenario is becoming even more critical to U.S. defense planners.

Currently, the U.S. maintains a position of "calculated ambiguity" on how it will respond to a CBRN attack on its soil or against its interests abroad. The doctrine of calculated ambiguity garnered support when the Bush administration purportedly deterred Saddam Hussein from using biological or chemical weapons against U.S. forces during the first Gulf War in 1991. Secretary of State James Baker delivered a note to Iraq's Foreign minister Tariq Aziz that cautioned Hussein that any use of these weapons could result in U.S. nuclear reprisals. The unclassified version of the 2002 National Security Presidential Directive (NSPD) 17 declares that the U.S. will reserve the right to respond with "overwhelming force" and keep open "all of its options" to a CBRN attack on the U.S., its interests, or its allies. In 2003, *The Washington Times* reported that the

classified version of NSPD 17 made the willingness of the U.S. to respond with nuclear weapons to a CBRN attack more explicit.[14] Nevertheless, the U.S. is deliberately vague about its plans to respond to a CBRN attack. The strategic rationale for maintaining this ambiguity is to keep open a broad range of response options and approach potential events on a case-by-case basis. The vagueness of U.S. reprisal plans, however, does not support deterrence. The credibility of U.S. threats to retaliate suffers as a result of this ambiguity. While the use of language such as "overwhelming force" connotes a severe retaliation, this lack of clarity is not the best way to solidify the belief among terrorist-supporting regimes that their behavior puts them at severe risk. As one author notes, "Frequently, the bigger and more indiscriminate the threat, the less believable it is in the eyes of the target audience."[15]

In order to establish a deterrent mechanism that will dissuade rogue states from supporting terrorist organizations, the U.S. must develop a strong declaratory policy that clearly communicates a threat of punishment for those states that provide CBRN materials to terrorists. Strategies for dealing with rogue states assisting terrorist organizations that are severe and target assets of value to the regime will best reinforce deterrent mechanisms. As Ian Lesser argues, for deterrence to be viable against rogue regimes, the threat of retaliation for supporting or sheltering terrorist organizations must be both "massive" and "personal to the leadership."[16] The U.S. policy of calculated ambiguity reinforces many of the internationally held stereotypes of the U.S. that negatively affect its ability to establish a credible deterrent threat. By avoiding direct language, the U.S. appears irresolute, noncommittal, and perhaps overly sensitive to public opinion.

To create a credible deterrent threat, the U.S. must articulate a policy of regime change in those states that offer support to terrorist groups. Regimes that assist groups such as al-Qaeda, especially if this assistance is with acquiring CBRN capabilities, must know that they will be toppled and replaced if this support is identified. Specifically, the leadership of rogue regimes must be explicitly warned that they will be removed from power, suffer legal repercussions, or even be killed for maintaining ties with terrorist groups. Doing so would represent a meaningful threat of punishment to the leadership of rogue regimes. However, a stated policy of regime change presents numerous dilemmas. Most notably, sovereignty is still a revered concept in international relations. Engaging in a war to bring about regime change is acceptable in the international community only in instances of clear self-defense or through the decision of the United Nations Security Council.[17] Thus, in order to have international support to carry out a regime change, the U.S. would have to bring forth evidence that a particular state was responsible for transferring CBRN capabilities to a terrorist group that carried out an attack on the United States.

Making the case for regime change in Afghanistan was easy, as it was fairly clear to the international community that the U.S. was retaliating against a regime guilty of harboring and providing sanctuary to al-Qaeda. However, future attempts to gain international approval for regime change may be more difficult than they were in Afghanistan. The failure to garner widespread international support for the U.S. invasion of Iraq and the subsequent failure to find CBRN weapons will only serve to make the international community more skeptical of U.S.-led efforts to topple rogue regimes. Furthermore, the difficulties the U.S. has had in "winning the peace" in Iraq will decrease the credibility of U.S. threats to dismantle rogue regimes. The ruling elite

in rogue regimes may be unconvinced of the willingness of the U.S. to topple a regime and engage in another nation-building effort. These arguments correspond with the often-heard suggestion that U.S. policy in Iraq has undermined its ability to fight the war on terror in other parts of the world.

In addition to articulating a policy of regime change, the U.S. must be more explicit in its capability and willingness to respond with nuclear weapons in the event of a CBRN attack. It remains uncertain whether the U.S. is likely to retaliate against an enemy that has used CBRN with either conventional or nuclear weapons. The psychological weight that the ultimate sanction of nuclear reprisals carries is critical in developing a meaningful deterrent threat against rogue regimes transferring CBRN capabilities to terrorists. As one author suggests, "The extremely high costs that a rogue state might suffer from nuclear retaliation should give even the most reckless of regimes pause before sharing a nuclear capability with terrorists."[18] Threatening a massive conventional weapon response simply does not carry the same deterrent weight as the threat of nuclear reprisals. However, current U.S. nuclear capabilities prevent the U.S. from convincingly threatening nuclear retaliations against rogue regimes. The U.S. nuclear arsenal is too destructive to consider using, other than in retaliation to a nuclear attack. Because the U.S. nuclear arsenal consists primarily of weapons that have yields of hundreds of kilotons, U.S. threats to use nuclear weapons, especially in response to a biological or chemical weapon attack, are too incredible for rogue regime leaders to take seriously. Ambiguous threats about leaving the nuclear option open, when many enemies of the U.S. maintain little belief that the U.S. is willing to take action on these veiled threats, fails to support deterrence. The U.S. cannot credibly threaten nuclear reprisals against a CBRN attack because it is perceived the U.S. would not risk the extensive collateral damage and civilian casualties that would result from using the weapons in its current nuclear arsenal. Rogue regimes may rely on this moral and political reluctance by the U.S. when they consider transferring CBRN capabilities to terrorists.

In order for the nuclear option to be a credible part of the strategic menu, the U.S. must continue research on, and eventually development of, low yield nuclear weapons. Next generation "mini-nukes" could theoretically engage targets such as underground command and control bunkers, weapon labs, CBRN storage facilities, or even a presidential complex. As U.S. operations in Afghanistan and Iraq have illustrated, the war on terror will often present high-value targets that cannot be efficiently engaged with conventional munitions.

The development of mini-nukes and subsequent establishment of a declaratory policy of nuclear retaliation is a potentially divisive issue. First, the 1993 Spratt-Furse law bans any research and development of nuclear weapons that have yields of less than five kilotons. In May 2003 the House of Representatives adjusted the law, allowing research on low-yield nuclear weapons, but stated clearly that development and production of these weapons remains prohibited. Second, the mini-nuke debate polarizes the positions of "deterrence hawks" and "nonproliferation doves." The production of mini-nukes blurs the line between nuclear and conventional munitions. It also creates a number of nuclear fallout concerns and undercuts U.S. counterproliferation efforts. For instance, the U.S. government, through the 1995 Nuclear Non-Proliferation Treaty (NPT) extension conference, assured that it would not use nor threaten the use of nuclear weapons against non-nuclear members of the NPT. Third, some scholars, notably Scott

Sagan, argue that explicitly threatening nuclear retaliation could lead to a "commitment trap" whereby U.S. officials may feel that they *must* respond to an attack with nuclear weapons in order not to "lose face" domestically and internationally.[19] Finally, since WWII, a nuclear taboo has emerged in the U.S. and throughout much of the international community, whereby a normative prohibition stigmatizes the use of nuclear weapons as something only done by "bad states." Therefore, some suggest that by producing nuclear weapons that are designed for non-nuclear targets, the U.S. may undermine the nuclear taboo.

A second important step in establishing a credible threat of retaliation involves CBRN weapon attribution. To effectively deter states from transferring CBRN materials to terrorists, the U.S. needs to develop its ability to identify the origin of the CBRN materials used in an attack against the U.S. The prospect of an unattributed CBRN attack poses a significant dilemma for establishing a deterrent mechanism. As Michael Levi argues, the U.S. must develop its ability to identify where the materials used in a CBRN attack originated. While intercepting weapon transfers before they occur should be the primary goal, the U.S. must have the technical ability to identify where CBRN materials came from *after* they have been detonated. As Levi points out, "If the United States can take that technical step, it can credibly assure its enemies that their transfer of weapons to terrorists will ultimately lead to their demise."[20] Without adequate attribution ability, rogue regimes may be more inclined to transfer CBRN capabilities to a terrorist organization because they believe their identity may never be revealed. As long as rogue regimes believe the U.S. cannot detect where CBRN materials originated, U.S. threats of retaliation are somewhat hollow.

While continued efforts by the Defense Department to develop a more robust attribution system are vital, the infancy of this capability requires the U.S. to make a much more controversial threat in the near-term. It is not certain that the U.S. will always be able to garner enough forensic evidence from a CBRN attack to pinpoint the origins of these weapons after an attack has been carried out. There is a lingering question of how compelling forensic evidence must have to be in order to justify a massive retaliation against a state suspected of providing CBRN assistance to a terrorist organization. To establish an effective deterrent mechanism the answer to this question violates accepted legal standards. The U.S. will need to be prepared to retaliate on the basis of limited or imperfect information about the origins of weapons material. That is, the burden of proof will have to be relaxed. As a recent RAND report conjectures, in the event of a CBRN attack the U.S. may be forced to retaliate based upon "…reasonable evidence and would even make some assumptions about who is supporting terrorists in possession of WMD."[21] U.S. retaliation would have to come in spite of there being some doubt about where the CBRN capabilities actually originated. A U.S. decision to retaliate against state targets based on imperfect information will undoubtedly fan anti-American flames around the world and may even generate substantial domestic dissent. This is especially likely in light of the fact that the current White House toppled Saddam Hussein's regime despite considerable questions about Iraq's CBRN capabilities and development programs. The Kay Report has raised serious questions about the existence of ties between Iraq, al-Qaeda, and CBRN.[22]

Attribution difficulties present another, even more controversial, issue in terms of deterring states from transferring CBRN capabilities to terrorists. In addition to threatening massive retaliation and regime change against state supporters of terrorism,

the U.S. must also develop a doctrine of retaliation against CBRN proliferators that do not adhere to international standards of securing CBRN materials. Even with the establishment of certain enticements through the Cooperative Threat Reduction (CTR) framework, or Nunn-Lugar legislation, a number of states have not developed the necessary safeguards to secure critical weapons materials. Pakistan and Russia, for example, continue to maintain fissile nuclear material facilities that are poorly secured. Moreover, the CTR and other nonproliferation efforts have failed to prevent Iran and North Korea from pursuing nuclear capabilities. A comprehensive deterrent strategy would also threaten retaliation against those states that jeopardize international security by not conforming to international standards of safeguarding CBRN materials. That is, the "mere" crime of negligence and carelessness in overseeing CBRN materials must be punished. This is especially true in the event the U.S. cannot identify the origin of CBRN materials used in an attack. The U.S. must clearly communicate its willingness to severely punish those states that, because of mismanagement of CBRN, risk the loss or theft of critical materials from their storage facilities. Such a policy stance would be extremely contentious and may damage the relationship the U.S. has with a number of states. However, until CBRN attribution becomes certain, to establish a meaningful deterrent mechanism against states that knowingly transfer sensitive materials the U.S. must also threaten those states that do not adequately secure their CBRN materials.

The above discussion illustrates that establishing a deterrent mechanism, even in the theoretically most applicable case of deterring states from supporting terrorist organizations, would require the U.S. to adopt a number of controversial policies. To establish a meaningful deterrent mechanism against rogue regimes from supporting terrorist groups, the U.S. must take the following steps: (1) explicitly state that the U.S. will dismantle and destroy any regime guilty of supporting terrorist organizations, (2) increase research and development of mini-nukes and clearly communicate its willingness to retaliate with these weapons in the event of a CRBN attack, (3) develop a robust CBRN attribution system, and (4) warn states that do not maintain adequate security over CBRN materials and weapons that they will be punished in the event the U.S. is unable to identify the origins of a CBRN weapon used in an attack. Clearly, a number of these policies would be unpopular to many around the world. The uproar generated by President Chirac's and Congressman Tancredo's recent comments illustrates the potential problems with articulating a policy of massive retaliation and regime change. Moreover, the U.S. cannot make a credible threat of nuclear retaliation to a chemical or biological attack because its current nuclear arsenal is comprised mostly of weapons that are far too destructive. Making a credible threat becomes even more difficult when retaliation may have to be carried out on the basis of incomplete information about who exactly was responsible for giving a terrorist organization CBRN capabilities. With the current difficulties of CBRN attribution, and the fact that a number of states that do not directly support terrorist activities are negligent in securing CBRN materials, the ability of the U.S. to communicate a clear and believable retaliatory threat is further hampered. There exists too much opportunity at the present time for rogue regimes to transfer CBRN capabilities to terrorists without detection and therefore without fear of reprisals. Until these opportunities are reduced, or the U.S. is willing to communicate and carry out a number of potentially unpopular policy choices, effectively deterring states from forming any relationship with terrorist groups is unlikely.

A final problem with deterring state sponsorship of terrorism is unrelated to the myriad of issues that surface in regard to CBRN weapons. One of the biggest difficulties policymakers and analysts face is that state sponsorship of terrorism can include a wide spectrum of actions and degrees – ranging from very passive to very active. Even more problematic is that some states that maintain some degree of support for terrorist organizations are loosely considered U.S. allies.[23] For example, Pakistan's intelligence service and military are known to sympathize with and at times directly support active Islamist terrorist groups in Kashmir. One such group, the al-Qaeda splinter group Jaish-e-Mohammed, has been linked to the December 2001 attack on the Indian Parliament and the 2002 murder of *New York Times* journalist Daniel Pearl. Therefore, to establish a credible deterrent mechanism, the U.S. would have to be willing to clearly signal to a number of its "allies" in regions such as the Middle East that it is prepared to carry out regime change or other drastic policy responses to even low-levels of passive support. Many countries, including purported U.S. allies in the war on terror, continue to "turn the other cheek" to terrorists operating within their borders because they simply do not believe or fear that the U.S. will punish them in a meaningful manner.

## Deterring Individual Elements

Beyond state supporters, other notable elements that comprise a terrorist organization may include financiers, recruiters, religious leaders, "foot soldiers," and the actual leadership of these groups. Deterring these actors is even more problematic than deterring rogue regimes from developing ties with terrorists. Deterring states from supporting terrorist groups would force the U.S. to adopt a number of potentially unpopular policy positions. However, the requirements to deter individuals within a terrorist system will force policymakers to compromise some very basic and sacrosanct American values.

The clearest example of this potential tension involves the issue of "targeted killings" of members of terrorist organizations. Targeted killings refer to operations carried out with governmental approval that seek to eliminate specific individuals who are considered to be serious threats to national security. A targeted killing differs from assassination in that assassination is the killing of a head of state or prominent political figure. Assassination is also a killing characterized by "treacherous" methods. In spite of this attempt at differentiation, the actual distinction between the two acts is largely a semantic one.

The issue of targeted killings has garnered considerable attention in recent years for a number of reasons. Israel has conducted targeted killings throughout much of its history. However, a wave of targeted killing operations carried out by Israel since the beginning of the second intifada in September 2000 has drawn increased attention to these methods. Israeli agents have recently used a variety of tactics, including car bombs, sniper bullets, helicopter gunship attacks, and booby traps, to kill individual members of Hezbollah and Hamas. Since September 11 the Bush Administration has also attempted to expand U.S. ability to target individual terrorist leaders and operatives. Administration officials argue that the U.S. must have more leeway to conduct targeted killings in order to punish members of an increasingly decentralized al-Qaeda organization. A main component of U.S. targeted killings has been the use of CIA-operated Predator drones. The January 13, 2006, Predator attack on targets in the Pakistani village of Damadola that sought to kill al-Qaeda's deputy Ayman al-Zawahiri

was especially controversial. The attacks failed to kill al-Zawahiri and reportedly left eighteen civilians, including five children, dead. Even Steven Spielberg's recent motion picture, *Munich*, about Israeli commandos hunting down and killing the Palestinians responsible for the slaying of Israeli athletes at the 1972 Munich Olympics, has thrust the issue of targeted killings into mainstream discourse.

The primary goal of the U.S. should usually be to arrest terrorist leaders and operatives. These individuals can be interrogated to obtain intelligence about other members of the organization and plans for future attacks. However, it is often too risky or even impossible to apprehend or capture terrorist operatives. If apprehending a member of a terrorist organization significantly endangers U.S. personnel, and there are no other feasible alternatives, then targeted killings are an option. Many Islamic fundamentalist groups are currently located in areas of the Middle East, Southeast Asia, Central Asia, and Africa where it would be dangerous for U.S. forces to try and apprehend them. A declared policy of targeted killing is vital, although controversial, to establishing a deterrent mechanism.

Some commentators have suggested that one of the main reasons that deterrence is irrelevant when it comes to fighting terrorists is that many of these individuals are prepared to die for their cause. Therefore, it is assumed that retaliatory threats of punishment mean little to individuals who are willing to give their lives in the first place. However, this reflects a narrow view of terrorist organizations. Besides suicide bombers, who may be impelled by the promise of martyrdom, other elements who comprise a group such as al-Qaeda are more risk-averse. Osama bin Laden, and other members of al-Qaeda's leadership, for instance, have not carried out suicide bombing missions nor attempted to engage U.S. forces in Afghanistan's mountains. Indeed, many members of al-Qaeda's leadership have literally been running for their lives since the September 11 attacks. Some analysts have pointed to the 2002 surrender of hundreds of members of the Palestinian Islamic Jihad to Israeli forces during large-scale military engagements in Jenin as evidence that many members of terrorist groups are not willing to give their lives.

Because the lives of individuals within a terrorist organization represents one of the few assets that the U.S. may be able to hold at risk, the U.S. must maintain the option of carrying out targeted killing operations. A declared U.S. policy of selective killings may compel terrorist leaders to consider the utility of engaging in terrorist activities. However, establishing an effective deterrent mechanism against potential actors will require the U.S. to be *much* more forthright in its intent to carry out targeted killing operations. It is essential that the U.S. explicitly affirm that it will kill members of terrorist groups that U.S. intelligence analysts believe are responsible for carrying out terrorist attacks against its assets or interests. The U.S. should also make clear that it will target members of a terrorist organization other than just senior leaders, such as those responsible for providing financial or logistical support to a terrorist organization. Broadening the scope of targeted killings beyond just senior leaders may serve to deter individuals who are merely "casual sympathizers" from committing to groups like al-Qaeda. To make these threats credible the U.S. should continue to seek and, when it cannot capture alive, kill all senior leaders of al-Qaeda who played a role in orchestrating the September 11 attacks. The U.S. has successfully tracked and killed a number of al-Qaeda leaders since September 11. However, to deter terrorism the U.S. must expand its capabilities to kill terrorist operatives. The Predator program

represents but one option the U.S. can explore to credibly threaten the lives of individual al-Qaeda members. Current political constraints, however, impede the ability of U.S. intelligence agencies and the military from carrying out focused covert operations to hunt down and kill terrorist transgressors. Until the constraints on these operations are relaxed even further, the U.S. will be unable to establish a deterrent mechanism that is functional, effective, and forthcoming with deterrent results.

While the morality of targeted killings remains a hotly contested issue, it appears that targeted killings do influence terrorists. Since 2002, for example, Palestinian leaders have repeatedly called for Israeli forces to cease carrying out these operations. On January 30, 2002, Israeli Prime Minister Ariel Sharon met with a number of Palestinian leaders. One of the primary demands of the Palestinian leaders was for Israel to immediately stop targeted killings.[24] Some analysts argue that targeted killings have been directly responsible for decreasing threats to Israel's national security. It appears that Egyptian terrorist infiltration of Israel in the 1950s decreased when Israeli agents killed the Egyptian intelligence officers who oversaw the operation. Retaliation against the Black September terrorists in the 1970s who killed Israeli athletes in Munich virtually destroyed the organization.[25] Since the beginning of the second intifada in September 2000, empirical evidence suggests that Israel's targeted killing campaign has been successful. As cited by Daniel Byman in his timely 2006 *Foreign Affairs* article on the efficacy of targeted killings, the National Memorial Institute for the Prevention of Terrorism reported that Hamas killed twenty-one Israeli civilians in 2005. This number was a fairly sharp drop-off from the sixty-seven who were killed in 2004, forty-five in 2003, 185 in 2002, and seventy-five in 2001. It is believed by many, especially in Israel, that Israeli targeted killings have "shattered Palestinian terrorist groups" and made it difficult for these groups to orchestrate large-scale suicide attacks.[26]

The individuals who actually carry out violent terrorist acts represent the most difficult group to establish a deterrent mechanism against. Unlike other members of a terrorist group, "foot soldiers" are often willing to give their lives for the organization's cause and achieve martyrdom. To these individuals, the prospect of dying "in battle" against the perceived *infidel* is considered a great honor. Therefore, threatening to kill these individuals would likely do very little to deter them from continuing to carry out suicide missions or other types of violent acts. However, achieving martyrdom is only part of the motivation for suicide bombers to give their lives; giving one's life in battle against the infidel results in monetary rewards for a martyr's family members. Many martyr's families are compensated with payments usually ranging between $12,000 and $15,000. Furthermore, significant psychological benefits are derived from a family member giving his/her life in these struggles. The act of martyrdom is considered a heroic deed and results in glorious funeral ceremonies and the immortalization of the individual through graffiti, portraits, trading cards, and other memorabilia.[27]

Because of the value martyrs may place on the monetary and psychological rewards that come to their families after their death, an effective deterrent strategy by the U.S. must include threatening to punish the families of suspected foot soldiers. Meaningful threats of punishment would include targeting either the lives or livelihood of these family members. In a recent article by Major General Doron Almog of the Israeli Defense Force, Almog gives a poignant account of a particular instance where Israel attempted to dissuade a potential suicide bomber by threatening his family:

> In early 2003 an Israeli agent in the Gaza Strip telephoned Mustafa, a wealthy Palestinian merchant in Gaza, to inform him that over the previous three months his son Ahmad had been preparing for a suicide bombing mission in Israel. Mustafa was told that if his son followed through with his plans, he and his family would suffer severe consequences: their home would be demolished and Israel would cut off all commercial ties with Mustafa's company. Neither he nor the members of his family would ever be permitted to enter Israel again. Faced with this ultimatum, Mustafa confronted his son and convinced him that the cost to his family would far outweigh any possible benefits his sacrifice might have for the Palestinian people.[28]

A better-known example is the alleged response by KGB agents for the September 1985 Hezbollah abduction of a Soviet diplomat. Reportedly, in retaliation for the abduction, KGB agents kidnapped and killed a family member of a senior official in Hezbollah. The KGB agents removed his genitals and stuffed them in his mouth before returning the body to his relatives. After the family of the deceased received his body, the Soviet diplomat was quickly released.

If the U.S. can remove the benefits that suicide bombers' families receive from carrying out an act of violence, it is possible that suicide bombers would be more hesitant to engage in that action. A more meaningful deterrent threat would include threatening to kill close family members of a terrorist operative who was identified as a perpetrator of violent acts against the U.S. or its interests. If terrorists truly believed their actions would result in the death or destruction of their family's way of life, it may deter some of them from engaging in or supporting terrorist violence.

Irrespective of whether targeted killings are an effective counterterrorism tool, the political, legal, and moral legitimacy of these operations are controversial. First, there is a history of various U.S. agencies coming under fire for supposed links to assassination programs. Most notably, the 1976 Church Committee put pressure on the CIA for its involvement in the Phoenix program, which attempted to find and neutralize Viet Cong members who were carrying out activities that attempted to destabilize South Vietnam during the war. The Church Committee directly confronted questions about how necessary strategic objectives reconcile with democratic ideals. The Committee concluded that "…assassination is unacceptable in our society" and that it "…was struck by the basic tension – if not incompatibility – of covert operations and the demands of a constitutional system." The Committee was most concerned with efforts to assassinate foreign leaders, such as Cuba's Fidel Castro; however, it is likely that many of the same arguments maintained by the Church Committee would emerge in regard to a clearly stated U.S. policy of targeted killing.

From a legal standpoint, targeted killings "walk a thin line." Assassination is prohibited, as a matter of national policy, by Executive Order 12333. This Order states that no person acting on behalf of the U.S. Government shall engage in assassination. However, this assassination ban provides considerable flexibility and is conspicuously imprecise. Targeted killings against legitimate targets who threaten U.S. national security, determined by the President, do not constitute assassination and are not prohibited by Executive order 12333. For instance, President Ronald Reagan authorized the attempt to kill Libya's Colonel Muammar Qaddafi for Libya's role in the 1986 bombing of a West Berlin discotheque. President Clinton also relaxed the constraints on targeted killings following the U.S. embassy bombings in East Africa. Clinton authorized

the use of cruise missiles against targets in Afghanistan and the Sudan in response to the attacks. Finally, the current White House has stated that it maintains the right to carry out targeted killings based on war powers granted to the president by Congress after September 11. Another complexity of the legality of targeted killings is the fact that these operations, under international law, cannot be carried out as an act of revenge or reprisal for a past event. Targeted killings are only legal if they are done in an effort to prevent a future threat to a nation's security.[29] Delineating actual revenge killings from killing someone to prevent future threats to U.S. security is a murky issue by itself. This is especially true when it comes to dealing with terrorist organizations that wage continuous campaigns of violence against an enemy.

A second dilemma for targeted killings involves the issue of national sovereignty. Targeted killings of terrorist leaders and operatives may violate the sovereignty of other states unless these killings are authorized by the state in which the killing takes place. Some analysts speculated whether Pakistan was informed of the 2006 Predator attempt to kill al Zawahiri in 2006 in Damadola.

A third concern about the U.S. engaging in targeted killings is the condemnation that these operations have drawn from members of the international community. Prior to September 11, even the U.S. was fairly vocal in its admonishments of Israel's targeted killing policy. In July 2001, Secretary of State Colin Powell stated, "We continue to express our distress and opposition to these kinds of targeted killings and we will continue to do so."[30] Following the 2002 Predator strike in Yemen that killed Ali Qaed Sinan al-Harthi, a leading al-Qaeda member and prime suspect in the 2000 attack against the USS Cole, many suggested that the Bush administration was moving away from the law-enforcement tactics of arresting and detaining terrorist suspects to a more controversial policy of targeted killing or extra-judicial killing.

Soon after the strike on al-Harthi, a United Nations report condemned the attacks. The report stated that the attack established an alarming precedent and was a clear case of extra-judicial killing and therefore a violation of international law.[31] Extra-judicial killing refers to the deliberate killing of an individual where it is deemed that apprehending and arresting a suspect is not a viable alternative. Similarly, Amnesty International claimed, "If this was the deliberate killing of suspects in lieu of arrest, in circumstances in which they did not pose an immediate threat, the killings would be extra-judicial executions in violation of international human rights law."[32] Other vocal opponents to targeted killings by the U.S. and Israel include many Arab and European Union governments. Sweden's Foreign Minister went so far to say that the Yemen strike was "…a summary execution that violates human rights. Even terrorists must be treated according to international law."[33] Because of the widespread condemnations of targeted killings, the perception of the U.S. as an upholder of the rule of law will diminish even more than it already has in recent years if the U.S. expands its operations in this area.

In addition to the legal and political repercussions of the U.S. engaging in targeted killings, a more fundamental issue about these practices arises. The U.S. must ask whether it wants to be a nation that is associated with targeted killings, assassinations, and threatening families of terrorists to establish deterrence. The U.S. has often turned to Israel to evaluate its own strategies to defend against terrorism. However, Israel is a different case altogether. Israel must approach counterterrorism not from a perspective of national security, but from a perspective of national survival. Israel constantly finds its society and its citizens' way of life under siege by Palestinian terrorists. Palestinian

terrorists who come from the West Bank and the Gaza Strip are only miles from Israeli territory.[34] This is not to diminish the threat that terrorism poses to the U.S., but what may be necessary for Israel may not be appropriate for the U.S. It must be considered whether a declaratory policy of targeted killings is fundamentally compatible with American core values and morality. This is not a question that should be conveniently dismissed as mere fodder for liberal editorial pages or grandstanding speeches by left-wing academics. It is a legitimate concern that even the most hawkish American citizens should at least reflect upon.

To be sure, a significant reason for the Bush Administration not coming under more fire than it did for calling for the capture of bin Laden "either dead or alive" was the widespread public outrage over the September 11 attacks. Therefore, as the memory of these attacks subsides and the country moves beyond these tragic events, it is unclear whether future administrations will be able to successfully convince the American public that targeted killings are reconcilable with the core values of the nation. Moreover, it is likely that a stated policy of punishing the families of suicide bombers or other terrorist operatives would be met with considerable criticism. Threatening individuals who are perceived to be innocent and are not guilty of collaborating in an act of terrorist violence would be morally repugnant to many, albeit an effective tool to enhance deterrence.

## CONCLUDING REMARKS

Returning to the theoretical core of classical deterrence theory illustrates the deterrence dilemma in which the U.S. currently finds itself. To deter terrorists, the U.S, must ask itself two questions. First, what can it do in response to a terrorist attack? Second, are U.S. enemies persuaded that the U.S. will actually do what it says it will do? This second question represents the "Achilles' heel" of U.S. terrorism deterrence. Since September 11 the U.S. has been resolute in its pursuit of terrorist perpetrators. However, has the U.S. fully persuaded terrorist organizations that it is willing and able to punish them for their actions? Do terrorist elements view current U.S. actions simply as an out-of-character "knee-jerk" reaction to September 11? Will U.S. resolve in the war against terror waver, as it has in previous wars and conflicts? How much do calls for the U.S. to police its own actions in regard to moral and legal considerations undermine its credibility to punish terrorist acts?

The nature of America's democratic system and the need for retaliation efforts to "pass moral muster" continually remind our enemies that they will rarely have to face the full consequences of U.S. power. To deter terrorists from attacking the U.S. or its interests, the U.S. will have to be prepared to compromise many of its core values and conceivably set in motion the moral decline of the world's lone superpower. In truth, many of our enemies must be amazed by some of the debates currently being waged in the United States. Debates regarding the humane treatment of suspected terrorist detainees, responding in a proportional manner to suicide bombings, upholding the civil rights of September 11 suspects, or not directly targeting terrorist perpetrators are most likely construed as superfluous discussions by U.S. enemies. Incidents viewed as symbols of U.S. heavy-handedness by some Americans, such as Guantanamo Bay or Abu Ghraib, may not represent the same thing to U.S. enemies. Robert Kaplan made this point recently: "For Iraqis meeting with Americans in Mosul, 'Abu Ghraib' had a

different connotation than it did in the United States. Here it meant not brutality but American weakness and lack of resolve."[35]

Concern over the cost of compromising our ideals undoubtedly undermines efforts to make our enemies believe we are willing to punish them no matter at what expense. To effectively deter terrorists the U.S. will have to accept the price that comes with violating some human rights, responding with overwhelming force, alienating certain allies, and even eliminating those assets and people that terrorists may hold dear. Any discussion of deterrence that fails to acknowledge the necessity to implement such policies belongs only in ivory towers where the theoretical does not have to be tested by the practical. Deterring terrorists will not happen with strong policy statements alone, it will only happen if the U.S. can clearly illustrate to terrorists and their supporters that they will feel significant pain as the result of their actions. However, as long as arguments about the conflict between what is necessary and what is right continue to resonate throughout American society, the idea of deterring terrorists, who have no qualms about using pipe bombs to blow people up, represents little more than a pipe dream. And even if we, as Americans, did suggest that we were willing to sacrifice some ideals to combat terrorists, would the terrorists believe us?

*Uri Fisher is a PhD candidate in the Department of Political Science at the University of Colorado-Boulder. He is currently completing his dissertation entitled "Military Entrepreneurship and War Duration."*

---

[1] Paul Davis and Brian Michael Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al-Qaeda* (Santa Monica, CA: RAND, 2002), xvii.

[2] See for example Robert F. Trager and Dessislava P. Zagorcheva, "Deterring Terrorism: It Can Be Done," *International Security* 30, No. 3 (Winter 2005/2006): 87-123.

[3] Interview of President George Bush, "There is no doubt in my mind," *The Washington Post*, February 3, 2001.

[4] Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1970), 3.

[5] Molly Moore, "Chirac: Nuclear Response to Terrorism is Possible," *The Washington Post*, January 20, 2006.

[6] F. Ugboaja Ohaegbulam, *A Concise Introduction to American Foreign Policy* (New York: Peter Lang, 1999), 72-73.

[7] Clifford Kupchan, "Real Democratik," *National Interest* 77 (Fall 2004): 26-37.

[8] Gerald Steinberg, "Rediscovering Deterrence After September 11, 2001," *Jerusalem Letter/Viewpoints* (Jerusalem Center for Public Affairs: December 2001): 467.

[9] The White House, "Address to a Joint Session of Congress and the American People," September 20, 2001.

[10] See Congressional Research Service, "Terrorism: Near Eastern Groups and State Sponsors, 2002," February 13, 2002, 37.

[11] Quoted in David Ignatius, "A Gaddafi Cover-up," *Washington Post*, October 26, 2004.

[12] Thom Shanker, "U.S. Analysts Find No Sign bin Laden had Nuclear Arms," *New York Times*, February 26, 2002.

[13] Owais Tohid, "Pakistan and its Proliferator," *Christian Science Monitor*, February 6, 2004.

[14] Nicholas Kralev, "Bush Signs Paper Allowing Nuclear Response," *Washington Times,* January 31, 2003.

[15] Avigdor Haselkorn, *The Continuing Storm: Iraq, Poisonous Weapons, and Deterrence* (New Haven: Yale University Press, 1999), 49.

[16] Ian Lesser, "Countering the New Terrorism: Implications for Strategy," in *Countering the New Terrorism*, ed. Ian Lesser, et. al. (Santa Monica: RAND, 1999), 129.

[17] Pascal Boniface, "What Justifies Regime Change," *Washington Quarterly* (Summer 2003).

[18] Jasen Castillo, "Nuclear terrorism: Why Deterrence Still Matters," *Current History* (December 2003): 427.

[19] Scott Sagan, "The Commitment Trap: Why the United States Should Not Use Nuclear Threats to Deter Biological and Chemical Weapons Attacks," *International Security* 24, no. 4 (Spring 2000): 85-115.

[20] Michael Levi, "Deterring Nuclear Terrorism," *Issues in Science and Technology* (Spring 2004).

[21] Davis and Jenkins, *Deterrence and Influence in Counterterrorism,* 40.

[22] See the testimony of David Kay before the House Permanent Select Committee on Intelligence, October 2, 2003, http://www.cia.gov/cia/public_affairs/speeches/2003/david_kay_10022003.html.

[23] An anonymous reviewer brought this point to my attention.

[24] William Safire, "Sharon Enters Armistice Talks," *New York Times*, February 4, 2002.

[25] Steven David, "Fatal Choices: Israel's Policy of Targeted Killings," *Mideast Security and Policy Studies* 51 (September 2002).

[26] Daniel Byman, "Do Targeted Killings Work?" *Foreign Affairs* (March/April 2006): 103.

[27] Adam Dolnik, "Die and Let Die: Exploring Links between Suicide Terrorism and Terrorist Use of Chemical, Biological, Radiological, and Nuclear Weapons," *Studies in Conflict and Terrorism* 26 (2003): 29-30.

[28] Almog changed the actual names of these individuals; however, he contends this a true story. Doron Almog, "Cumulative Deterrence and the War on Terrorism," *Parameters* (Winter 2004-2005): 4.

[29] Amos Guiora, "Targeted killing as Active Self-Defense," *Case Western Reserve Journal of International Law* 36 (2004): 329.

[30] Quoted in "Cool Reception for Sharon in Europe," *BBC News-Online,* July 21, 2005, http://news.bbc.co.uk/1/hi/world/middle_east/1424911.stm.

[31] Josh Meyer, "CIA Expands Use of Drones in Terror War," *Los Angeles Times,* January 29, 2006.

[32] Anthony Dworkin, "The Yemen Strike: The War on Terrorism Goes Global," *Crimes of War Project* (November 2002), http://www.crimesofwar.org.

[33] Quoted in Max Boot, "Retaliation for Me, but Not for Thee," *The Weekly Standard,* November 18, 2002.

[34] Daniel Byman, "Do Targeted Killings Work?" 107.

[35] Robert Kaplan, "The Coming Normalcy?" *The Atlantic* (April 2006), 78.

# Interoperability: Stop Blaming the Radio

Ronald P. Timmons

## INTRODUCTION

One of the most pressing first responder issues emerging in the post-9/11 era is the need to improve emergency scene radio communications.[1] This concern actually pre-dates the terrorist attacks on the United States in 2001, and has been a commonly cited issue, in dealing with nearly every disaster or incident of major significance, for many years.[2]

The one word repeatedly heard in describing the problems relating to disaster scene communications is "interoperability." Without full consideration of all the causal factors, the charge has been to fix the oft-cited frustration of field responders being unable to communicate – and all the blame has gone to interoperability. The 9/11 attacks were a catalyst for an unprecedented amount of money spent on radio hardware. The numbers are staggering: estimates range up to five billion dollars in homeland security grants to enable and facilitate emergency communications.[3] Hurricane Katrina in 2005 again sent first responders looking for communications improvements.[4] This article challenges first responders to look beyond technical solutions and consider other factors impeding emergency scene communications.

Defining the issue has been difficult. Is *interoperability* the ability of all police officers to talk on radios to all firefighters at the same incident? Does interoperability refer to federal agencies having radio connection to state and local officials? Is interoperability only for those at the scene, or command post, or for those at the Emergency Operations Center as well? Will it be provided for every responder or command-to-command only? Or does interoperability address the wider issues of radio system coverage, frequency spectrum capacities, technology piece ergonomics, and alternate (non-voice) communications methods? Interoperability has been used as a catch-all phrase to describe a multitude of issues surrounding emergency scene communications. There are numerous reasons for inadequate disaster communications. Nationwide efforts, such as the Department of Homeland Security's Project SAFECOM, have begun to acknowledge an expanded definition of interoperability beyond the technical, to include behavioral and procedural elements.[5] Communication impediments do include insufficient radio infrastructure, but they are also influenced by behavioral reactions of first responders in stressful situations, dysfunctional intergovernmental relations, inadequate procedures and training, and general lethargy over the need to institute special operating policies differing from routine habits and practices.[6]

The early homeland security grants approach, immediately following 9/11, was to deploy equipment to patch radio systems and devices together, or purchase more individual radio units to communicate over obsolete and inadequate radio systems. The result has been the expenditure of huge sums of grant dollars on communications patching equipment, perhaps creating the mistaken impression

on the part of first responders that emergency scene communication will instantly and automatically be improved once the equipment is bought and plugged-in.[7] Before efforts such as the SAFECOM Program, "…interoperability efforts were uncoordinated and spread across a variety of Federal agencies." Total reliance upon technological solutions, without proportionate training and practice, greatly reduces the effectiveness of radio patching equipment.[8]

New radio gateway patching equipment was deployed nationwide, with little initial guidance or consensus for proper use. Since then, planning and training components have been introduced into the grant process and major urban areas have been compelled to file and test Tactical Interoperability Plans in 2006, but the migration of theory and specific manipulative skills, down to the user-level, has been slow to occur.[9] A major interoperability survey, just released, found that "…strategic plans for interoperability are the exception rather than the norm."[10]

This article suggests alternatives to overzealous equipment interconnection and instead urges a rethinking of the factors faced by personnel operating at a disaster. Common practice and policies should include new procedures for first responders when using radio equipment designed to improve interoperability. Communications improvement alternatives, such as training responders to prioritize radio traffic and employ alternatives, should be carefully weighed and tailored by first responder policy makers, while devising a policy best suited for their local jurisdictions.[11]

## OPERATIONAL REALITIES

Beyond the mere technical aspects, policy makers need to consider the complexities facing those operating at the scene of emergencies. The radio is one tool of communication, but the overall process of communications deserves greater attention.

The daily routine of first responders does little to prepare those responders for the communications-intense environment typical of large scale disasters. Yet the universal reaction of response personnel at after-action reviews has been shock and indignation over failed communications at disaster scenes, followed by a tendency to blame the equipment instead of the people. The *9/11 Commission Report* goes into great detail about the failings of the radio systems of various agencies responding to the terrorist attacks in New York City in 2001.[12] Transcripts and recordings reveal there was almost constant chatter, albeit sometimes choppy and unintelligible. Setting aside the technical issues, which were many, a lot of people still talked on the radio; so while much was being *said*, *communication* was weak. More recent exercises have identified similar shortcomings. The observations and recommendations emanating from the civil-military *Strong Angel* exercise series echo many of the same frustrations about communications inefficiencies and recommendations for new ways of providing communications support.[13] The challenge will be in getting new concepts understood and accepted by the individual first responders in the field. Large-scale emergencies challenge the first responder community to find new ways to prepare personnel for situations that will be uncomfortable, unfamiliar, and

counter-intuitive. While there are steps that can be taken to stretch the communications resources deployed at emergency scenes, the logical approach is to manage the input (the amount of radio talking done at the scene) as well.

First responders tend to revert to normal usage habits in times of crisis, instead of modifying their use of the system when many agencies have been patched together, increasing system overload. The net result is that daily radio practices are accelerated and multiplied, with a dramatic increase in the quantity of communications by the responders at an incident, *and* these communications are squeezed into limited communications systems. The Department of Homeland Security (DHS) encourages first responders to "use interoperability solutions every day," so that "coordinated communications in response to any incident will be a natural instinct."[14]

Traditionally, there has been a tendency to devise hardware solutions for a whole range of challenges, instead of addressing human engineering issues.[15] The desire for a "turnkey" solution is understandable; the purchase and delivery of new equipment signals tangible evidence that something is being done. Considering that the kind of cataclysmic incidents we are preparing for are infrequent and the statistical exceptions, it is difficult to thoroughly assess the effectiveness of new equipment and procedures, even in the most realistic training exercise environment. Careful insight and informed projections are needed to ensure we do not find ourselves in the same state of dysfunction ten years from now, because we bought the equipment but did not change our culture and habits.

Funding for training accompanies some interoperability grant programs (signaling recognition of the importance of attention to non-hardware solutions) yet specific examples of actual training applications are difficult to find. What constitutes "interoperability training" is vague and nonspecific, leaving room for the requesting jurisdiction to include the component in their grant application while excluding specifics. Once agencies recognize the value of training to compliment the equipment they have deployed, training packages planned by DHS in the 2007-2011 planning window should facilitate those so inclined to participate.[16] To date there is disproportionately little collective recognition of the need for improved human interoperability communications procedures, as some first responder agencies presumably expect an out-of-the-box solution, based on building more communications infrastructure and patching radio systems together.

## PHYSIOLOGICAL INFLUENCES

It is helpful to briefly step back from the radio hardware focus and consider the theater in which personnel responding to a disaster operate. Examination of psychological and human factors demonstrates that the most robust radio system imaginable may not deliver the expected results.

## Sensory Overload

A lot is going through the minds of incident command personnel at the scene of an emergency; the amount of sensory input the brain has to process is immense. Just the process of *responding* to the incident in emergency mode takes a toll on the individual. First responders (in contrast to those working in stable environments) may be emotionally compromised when they arrive at the scene, before they are even called upon to perform critical decision making and clearly articulate commands to others.

When asked to describe the process by which emergency decisions were arrived at, a firefighter in one study indicated that he was not even aware that he *was* making a decision; it was more of a reflexive reaction than a conscious contemplation of a range of options to be selected from.[17] This is sometimes referred to as intuitive decision making and it reflects that people who are experts in their domain may react automatically without conscious thought and in the absence of full knowledge of the operational picture. More research is needed to determine the level of influence sensory overload and myopic operational tendencies exert on first responders expected to communicate in an optimal manner.

## Cognitive Bias

Another consideration is the tendency to apply "cognitive biases," a state in which people tend to discount information that disconfirms their (correct or incorrect) preconceptions.[18] This can lead to the incomplete or inaccurate relay of key information due to missing pieces of the operational picture, further confounding effective communications. Decision makers are susceptible to cognitive biases when operating under stress, i.e., high workload, time pressure, and information ambiguity.

## Speech Center Deficit

People within the first responder community can readily identify with the problem of speech center deficit, a phenomenon that sometimes occurs when someone is transmitting on a radio at the scene of a critical incident. Further study is needed to understand the role of hormone secretion, such as adrenaline and cortisol, plus other stress-related physiological reactions, which alter the voice pitch and inflection when someone is talking on the radio during a serious incident. As anyone who has listened to the famous recording of a reporter describing the crash of the Hindenburg ("oh, the humanity!") can attest, stress causes the human voice to take on a very unique quality, and the speaker can literally succumb to a state of "speechlessness."[19] Another example was Walter Cronkite's 1963 announcement of the assassination of President Kennedy, his voice cracking with emotion, as he was the first to break the story.[20] Mr. Cronkite did not witness the event, yet the weight of the information on a piece of paper caused an involuntary reaction influencing his speaking ability.

Recognition of this reality will allow us to scale back our expectations of effective voice communications at intensive emergency scenes. Responders should seek alternative communications methods and utilize message prioritization, for maximum value and improved operations.

### Suppressed Emotions

Another major influence inhibiting clear communication is a state of *expressive suppression*, defined as "consciously inhibiting emotional expressions while emotionally aroused."[21] First responders force themselves to "stay calm" and control the emotion in their voice. Review of incident recordings reveals that staying calm is critical to maintaining orderly radio communications, yet it can trigger a cascade of additional stressors for those involved.[22]

One study found that when people suppress natural emotional responses, they experience elevated blood pressure, increased stress levels, disrupted communications, reduction in rapport building, and inhibited relationship formation.[23] These byproducts are hardly a recipe for articulate communications and collaborative resource deployment with other agencies.

## LIMITATIONS INHERENT IN THE EMERGENCY ENVIRONMENT

The average incident commander generally arrives at the scene of a community emergency with little more than a portable radio and perhaps a clipboard of some sort. The largest first responder departments in the country may deploy drivers and aides with command officers, but they are the exception to emergency responses made nationwide. Command assistance, support, and technology are usually deployed on-scene as an incident escalates, but the capabilities to fund, staff, configure, and operate under pressure vary greatly across the country. While the level of support eventually brought in to a large-scale disaster provides assistance to the solo incident commander, it is during the first few minutes of a disaster that the incident commander is responsible for a wide array of critical duties and the chance for saving lives and preventing further consequences is greatest.

Once the influences affecting first responders are better understood and accepted, emergency trainers and planners are directed to several logical conclusions:

- There will be factors beyond the control of those present at the scene, impacting their ability to use radios in optimal ways. While training and experience can improve radio practices, particularly intense incidents (such as those where people are critically injured, awaiting rescue, or actively threatening others) should be anticipated, along with the propensity of those involved to be impacted emotionally. Emotional handicap should be anticipated in dire command circumstances.

  During periods of high-volume, high-stress crisis situations, the user's expectation of and reliance on good communication continues, but the increased pace and load on the radio system, combined with the unique

emotional influences present, typically acts to hamper, rather than facilitate, the communications process.

- Radio communications during cataclysmic events will not be as expedient or helpful as during lesser emergencies. People are creatures of habit and tend to revert to practiced behaviors in times of crisis. The same talkative practices used during daily, routine operations quickly collapse under maximum radio system loading.

  During periods of routine operations, confidence in using the radio equipment increases. The user generally has clear air for conversations with coworkers and dispatchers, communicating through casual or routine turns of speech. With light radio traffic and normal emotional states, first responders are able to conduct efficient business conversations on a daily basis. Nothing in this pattern adequately prepares the user for greatly accelerated and congested crisis communications.

- Consider how common it is for a member of the general public to feel apprehensive about delivering a routine speech to a large room of people, even with adequate notice and preparation. Then juxtapose the challenge inherent in disaster scene communications that requires verbalization, (ideally in optimized, unambiguous syntax) of a pattern of words containing specifics about an emotionally-charged emergency situation, the details of which were unknown just minutes prior. This helps to explain the dysfunctional communications experienced by disaster scene radio users.

- Personal protective equipment (PPE) tends to hamper access to and utilization of radio equipment. Despite improved equipment designs evolving over the years, this continues to be a factor. In addition, many non-firefighting personnel have been issued PPE through homeland security grants, but have never tried to use their radio equipment while wearing it.

The most well-intentioned plans and procedures can look very good on paper and fail to translate into valuable guidance during times of crisis, unless the limitations of the human physical and cognitive functions are considered. It is wise to anticipate the physiological limitations experienced by people under stress, and devise practical work-arounds to allow some level of prioritized communications to occur.

## Emergency Communications Under The Microscope

Accepting the aforementioned limitations inherent in emergency communications, we can benefit from detailed study of communication habits of first responders. Metrics obtained through radio system loading data provide valuable confirmation or counterpoint to anecdotal experiences reported by participants during routine incidents and training exercises. Decidedly less scientific, but nonetheless valuable, are user comments gleaned from after-action

reviews, during which communications issues are frequently discussed. Opportunity to quantify improvement needs can be identified in post-incident transcript reviews, during which the effectiveness of communications can be rated.

Transcripts and recordings from numerous critical incidents involving various combinations of fire, police, medical, local, and mutual aid units, responding to single and multi-jurisdictional incidents, were analyzed while conducting thesis research at the Naval Postgraduate School.[24] This included assessing incident transcripts from New York City on September 11, 2001, for timely and effective delivery of messages. Radio communications from a multi-jurisdictional fire department training exercise were evaluated in detail, revealing several opportunities for non-technical improvements.

Analysis of data from the training exercise communications studied showed the percentage of radio messages needing to be repeated was 4.9 percent. Another 11.9 percent of the radio messages went unacknowledged (thirty-three out of the fifty-one unacknowledged messages were to the incident commander), and were presumed to be unheard. In addition, 2.6 percent of the communications turns were judged to be a questionable use of radio airtime, e.g. face-to-face message exchange may have been more appropriate, the speaker was communicating redundant information, or information of questionable value was transmitted.[25]

Since radio system congestion is a commonly reported frustration, it is critical to find ways to make more airtime available. The collective total of repeated, unacknowledged, and questionable communications turns in this exercise equaled 19.4 percent of all messages, indicating a significant opportunity to reclaim nearly one-fifth of all radio airtime lost to such inefficiencies.

Unacknowledged messages to the incident commander are an area of concern, and were universally noted in training exercises, as well as in the recordings of actual emergencies. Further research is needed to fully assess predominant reasons for such inattention, since radio problems and clarity of the message were not typically noted on recordings. The incident commander was presumably distracted, overwhelmed, or attending to something else at that instant.

## HOW TO MAKE IT BETTER

One way to improve the communications efficiency rating is to provide training on better prioritization of radio messages while introducing the concept of communication alternatives to public safety radio. Face-to-face communication and decentralized emergency scene, sector-level, task coordination are examples of ways to achieve objectives without use of radio resources. Modifications to the status quo will be needed before the next major leap in emergency scene communications efficiency can be achieved.

### New Scene-Command Paradigms

Recognizing the intensive communications needs for efficient emergency scene success, we should strive to find new and better ways to provide a support system for first responders at the scene. New technology holds the promise of better emergency scene communications support, but it will require examination of how personnel are deployed and operate during an emergency. Over the last two decades, some large first responder departments have begun to transition to a fixed base of command operations at large emergencies, moving command personnel from literally standing in the street, to vehicle or building-based command posts. Homeland security grant dollars have facilitated the purchase of command post vehicles for many jurisdictions, yet there is general inattention to the need to prepare staff to optimize such resources. Mobile command facilities provide a greater array of communications support, beyond that which can be dependably delivered over handheld, portable equipment. It admittedly takes time and personnel resources to deploy such assets, so there is a need to start with operations more limited in capability, but the eventual deployment of enhanced capabilities will be of assistance in extended operations.

It would be beneficial to assign personnel at the emergency scene exclusively to facilitate communications support for the incident commander. Some large first responder departments have such scene-based communications capabilities (aides, chiefs' drivers, etc). Other agencies should seek creative ways to develop such expertise, perhaps detailing first-arriving support personnel (who often self-dispatch to large-scale incidents), or deploying special tactical dispatch personnel. Greater operational efficiency, enhanced crew safety, and "reclamation" of scarce radio airtime can be expected if communications support personnel operate inside a quiet environment, at the command post, with the incident commander. Communications specialists should be supplied with adjunct devices, such as headphones and visual displays, allowing them to pay close attention to radio traffic and data streams, thus assisting the incident commander in communications continuity.

## NIMS-The 10,000 Pound Elephant

In the recordings reviewed, considerable airtime was consumed in coordinating agencies. It was often apparent that separate commands were being employed at the same incident. The federal government has mandated the National Incident Management System (NIMS) as a condition of grant funding.[26] While many agencies claim to know and use NIMS, evidence of its field application is weak, especially in relation to multi-agency command from a single incident command post. Jurisdictions claiming to be enthusiastic adopters are often hard-pressed to show application of sound incident command and NIMS principles at emergency scenes ranging in complexity from the New York City attacks on 9/11, involving two 110-story buildings, to more routine traffic accidents and building fires.[27]

The reasons for slow or no adoption of NIMS range from traditional resistance to change, to a state of general denial of the possibility that large-scale emergencies can happen in any given jurisdiction, to what may be the biggest factor of all: a reluctance to answer the "who's in charge" question amid historic

turf battles, especially those related to police vs. fire department rivalries, and/or squabbles between various levels of government. Cordiality between agencies on the surface can belie the lack of NIMS application in the field.

Full implementation across all disciplines and jurisdictions will need to happen before optimum value is derived from the NIMS edict. A centerpiece of the new procedure involves dividing the incident into manageable pieces, with command officers assigned to task and/or geographical locations. These commanders can assume considerable line-of-sight and face-to-face communication with people in the task groups, thus eliminating much of the radio traffic at a critical incident. While the fire service has universally practiced incident command system principles for many years, law enforcement and other agencies have significant work ahead in transitioning from superficial, on-line NIMS overview training to effective, specific, and tactical NIMS implementation.

The *Unified Command* concept within NIMS is optimal when commanders from each agency are present at the same incident command post. While the separate command post concept is the practice in many locales, it probably has more to do with avoiding the "who's in charge?" issue than it does with any practical advantage. Unified Command is much more difficult when communications devices must be relied upon, instead of the optimal communications method: face-to-face.

## Governance

Some attention is starting to be paid to non-technical interoperability issues, including common governance and procedural recommendation.[28] But the most recent round of field tests revealed there is more work to be done in that regard. One U.S. Department of Justice official recently commented that governance is the greatest gap being found in field testing of interoperability initiatives.[29]

The drive for greater interoperability of radio communications has triggered more inter-agency collaboration, but there remains a need for greater control and governance over the use of interoperability equipment. While many jurisdictions have some history forming an alliance with a neighboring jurisdiction, it is rare to see all neighboring jurisdictions participating equally, and to see cross-jurisdictional policies (police/fire, local/county/state/federal, etc.). With the hardware now available to form ad hoc communications networks, agreement on common boundaries of utilization will be critical; otherwise inadvertent system overload is likely.

## Standardized Nomenclature

Interoperability initiatives have brought additional focus on the issue of agency-specific codes used over radio systems. Valid concerns have been raised about the presence of non-standard and often conflicting codes being used by many jurisdictions, along with the potential for critical errors in times of crisis communications. While some departments have phased-out radio codes in recent years, others still cling to them as an ingrained operating practice and custom.

The International Association of Chiefs of Police (IACP) recently addressed the Department of Homeland Security's (DHS) posture that 10-codes and other codes used over radio systems should be eliminated during daily use within the NIMS implementation initiative. At the 2005 annual meeting of the IACP, DHS Secretary Michael Chertoff yielded to the hue and cry of the membership to leave everything alone, as it relates to radio codes.[30]

This offers further evidence that we have a major "uphill battle" regarding any substantive changes to customs and traditional operating policies, even when the compelling need to overturn an existing practice is evident.

### Hand Piece Ergonomics

Often the radio itself is blamed, when operator error is really the cause. Public safety radio users frequently are not able to do much more than turn the power on, adjust the volume, push to talk, and maybe change a few channels. These users, like many people, may exhibit the "Blinking 12 syndrome," using only a portion of a technology product's capabilities (like the blinking, unset clock on home video equipment,) instead of reading instruction manuals and experimenting with seldom-used features.

The challenge for the future will be to configure radios to be more intuitive to use, while providing more training (and a commensurate level of motivational self-interest,) to the field responders who will need to know how to use their radio as a life-safety device, and during infrequent circumstances, immediately recall how to change to another bank of channels. Manipulating portable radio settings is a difficult task to accomplish under ideal conditions; the chance of successful selection of a different channel bank is much more challenging under stressful, adverse operating conditions.

### Data Displays

Given the limitations of delivering voice communications at intense incidents, a potent possibility resides in providing non-voice data to operational commanders. Incident recordings confirm that precious airtime is often consumed just to relay to incident commanders lengthy lists of units responding to the disaster. Because of the way data is transmitted over communications systems, more data can be delivered (within the same amount of airtime) than a commensurate amount of voice communication. Using more data transfer, as an alternate to some voice information, reserves the most intuitive and valuable form of communication – voice – for the highest priority messages.

## NEW PROCEDURES NEEDED

Specific procedures necessary to derive maximum benefit from the new interoperability equipment being deployed for homeland security communications improvement need to be addressed. Communications procedures should include teaching ways to economize use of communications assets, by placing priority on life-safety radio transmissions and practical, non-

radio alternatives for communicating during emergencies. Improved procedures should address application of NIMS incident management principles emphasizing the use of staging areas, sector control by assigning functional units under the control of a sector command officer, and application of face-to-face communications practices.[31]

In reviewing numerous recordings of critical incidents, it is apparent that the best practice would involve modification of radio system utilization, at the source, to optimize the quality of communications to produce "better" not "more" communications turns. Such a "less is more" posture, involving radio system use, runs counter to the policies practiced in daily response to routine incidents. All users must make a conscious effort at disaster scenes to resist the habits practiced in normal operations and limit their use of the radio system for the highest priority life and safety needs.

To overcome the inherent limitations of patching multiple radio system units onto a common operational platform, new procedures should be implemented to prioritize the use of limited radio resources. Review of numerous critical incidents involving various combinations of fire, police, medical, local, and mutual aid units, responding to single and multi-jurisdictional incidents, found a common pattern of influences:

1. Responding units tended to stop at the first injured person encountered at the periphery of the incident and call for an ambulance to that specific location, even when it should be obvious that a mass casualty incident was underway, involving dozens, or even hundreds of victims.
2. Turns of communications devolved into clipped, ineffective bits, to the point where it was difficult to tell who was talking to whom.
3. If a field unit expressed vocal excitement, the dispatcher's voice tended to also rise in pitch and pace. The dispatcher plays a key roll in keeping everyone calm through the use of a controlled voice inflection and by exuding a stoic confidence.
4. Units prefacing their transmissions with key words, such as "urgent" "priority message" or "emergency traffic," received greater attention than those continuing to talk unacknowledged and without preface, even if they conveyed urgency in the pitch and pace of their speech.
5. Many incidents eventually got to the point where dispatchers and incident commanders tried to control and reduce the volume of radio traffic by who was talking. Requests such as "all units stand-by" and "command officers only on this channel," were commonly heard.
6. A relatively small number of units dominated a majority of the airtime, often with non-critical matters, while many units said nothing. The channel-loading was unevenly skewed to a small portion of those present.
7. The most assiduous dispatchers and commanders tried to anticipate those things the field users might ask, and acted to broadcast a summary of

information, before it was asked for, in an effort to preempt use of the radio channel for repetitious information requests. This included best access routes, staging areas, triage points, command post locations, and brief situational updates. This relatively small menu of variables produced a disproportionate number of repetitious and superfluous radio transmissions.

8. The use of timed milestone updates gave the most even flow of information, acknowledging that time often gets out of phase – either faster or slower – to the perception of those involved at the scene. Many dispatch computer systems have automated features to trigger prompts to the dispatcher at timed intervals, i.e. every ten or twenty minutes. Dispatcher-initiated requests for updates from incident commanders, at timed intervals, aided in developing an operational picture for those at the scene, as well as for support players off-site (still responding, or at alternate locations, such as Emergency Operations Centers).
9. Listening to recordings after an incident readily allows for identification of inappropriate assumptions, ineffective ("not what was meant,") communications, and unacknowledged speech turns not evident to those involved at the moment. This can be attributed to the calm environment the reviewers are in and the lack of multi-sensory stimuli experienced by those responding as the incident was actually occurring. While it is not possible to eliminate all distractions and simultaneous demands placed upon those operating at emergency scenes, the inference here is that great value would be derived from managing and limiting sensory input at the scene.

## Quantifiable Triggers

Incident recordings reveal common themes in the contention for airtime: requesting individual resources unit-by-unit instead of in large task-force complements, and making requests that are relatively minor in contrast to the overall operational situation at hand.

There is a need for commanders of future cataclysmic events to monitor quantifiable triggers, such as:

- number of victims,
- area involved,
- configuration of structures, and
- type of attack methods used.

These cues can predict the impending overload of communications resources.

Such events should compel (via written procedure, training, and practice) the use of alternate communications tactics and contingencies. The "walking wounded," for instance, should be encouraged to keep walking or redirected to a central treatment area and radios should be used for priority messages only. Such

strategic use of radio systems during disasters has not generally been part of first responder orientation and training to this point.

## CONCLUSION

Homeland security efforts have been heavily focused on interoperable radio communications for local emergency responders. Recent homeland security dictates have listed interoperability as the number one focus for those seeking grant funding. The whole realm of communications behaviors needs to be considered, along with technical considerations.

Post-disaster analyses, including the *9/11 Commission Report*, have described a common frustration with ineffective communications at the scene of emergencies.[32] Assumptions made by the misinformed general public, as well as by some public-sector policy makers, have led to misguided solutions. Some solution strategies currently being pursued may actually make matters worse, instead of better (overloading systems by patching too many users together), despite billons of public dollars awarded through grant funding to *improve* communications.

The early assumption was that first responder communications issues were technical, i.e. separate radio platforms, or coverage issues leading to ineffective emergency communications. Such assumptions have a degree of validity, but the predominant focus should shift to procedural and human factors, considering the realities of how people perform during times of stress, rather than how to patch more radios together. Reviews of public safety radio transmissions during disasters, including the terrorist attacks of September 11, 2001, reveal a mélange of words and excited phrases that are often conflicting, disconnected, or superfluous.

Emergency scene communications dynamics are inherently complex because many diverse organizations become involved. A high degree of pre-incident diplomacy is necessary to create the governance process needed for such unprecedented levels of interagency collaboration required by the interoperability movement.

The greatest need is to modify procedures and behaviors, both in daily use and during disaster operations. We need to retrain field personnel in optimal radio operation procedures aimed at prioritizing radio transmissions for life safety, overall situational awareness status, and broad command and control.

Due to the criticality of communications during crisis events, it is imperative to devote resources to developing and implementing new procedures for responders during emergencies. This serves to increase awareness of the need to communicate differently in overload situations, instead of following the typical practice of loading more and more radio traffic into common radio space, to a point where communications turns are not accomplished and responder safety and effectiveness is impaired.

Communications are most critical during the response phase of an emergency. During the response phase, life safety matters are typically at their most acute state. Responders must deal with people awaiting rescue and treatment, while

focusing on apprehension of the perpetrators, damage assessment, and general situational status reporting. The stress of these missions tends to produce emotionally charged communications during the first hour of the incident, before elaborate field support systems can be established.

Since people revert to practiced behaviors when confronted with stressful situations, it is critical that the tendency of first responders to talk too much during an emergency be corrected. Spending more time listening to what is being said and saving the precious radio spectrum for prioritized life-safety-traffic-only communications is essential – and represents a new policy that needs to be taught and practiced. This will require specific guidelines, training, practice, and application by first responders and public safety communications personnel.

A *crisis communications plan* is advocated whenever command is established at the scene of an emergency where a large number of responders are present, and radio communications are beginning to degrade. Features of this plan should include:

- Encouragement of face-to-face communication within NIMS sectors;
- Designation of staging areas (where responders are directed to muster before deployment in the hazard zone), assigned by the incident commander, where units report and return silently to staging officers at those locations, without radio usage;
- Establishment of a dedicated communications path limited exclusively to the incident commander for situation status reports and requests for additional resources from/to dispatch;
- Coordination of command and dispatch to broadcast situational status reports at regular intervals; and
- Broadcasting to field units that life safety messages are to be prioritized, and they are to use other communications means for minor matters.

These modifications sound easy, even self-evident, but it is very difficult for people faced with a crisis to do anything other than what they have practiced in routine, daily operations. The recommendations made here represent a realistic set of alternatives for addressing the complex set of communications behaviors and influences present at disaster sites. These recommendations include engineering communication assets to fit the way first responders will likely react in emergency situations and introducing the new interoperability hardware with a commensurate level of relevant procedural changes and practice. First responders expect their communication issues to be fixed by radio hardware, yet strategic planning efforts show us it is time to shift the focus to human factors engineering and realistic acknowledgement of the limiting factors inherent at emergency scenes.

*Ronald P. Timmons, fire chief (ret.), Ridge Road Fire District, Rochester, N.Y., is presently the director of public safety communications for the city of Plano, Texas. He holds an MPA, and*

*earned a master's degree at the Naval Postgraduate School's Center for Homeland Defense and Security. He is pursuing a PhD in public affairs at the University of Texas at Dallas.*

The author gratefully acknowledges the contribution of his thesis advisory, Susan G. Hutchins, Research Associate Professor, Department of Information Science, Graduate School of Operational and Information Sciences, Naval Postgraduate School, Monterey, California. Her guidance and collaboration played a major role in the final version of this article.

---

[1] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton & Company, July, 2004), 280; Eileen Sullivan, "Interoperable Radios for First-Responders Woefully Lacking Despite Billions in Funding," *Congressional Quarterly* (September 2006), http://public.cq.com/public/20060911_topten_interop.html.

[2] "One of our biggest problems was communications," FDNY Assistant Chief Donald J. Burns, chief of operations, stated after the 1993 bombing of the World Trade Center. Chief Burns returned to the World Trade Center on September 11, 2001, and lost his life while commanding personnel under similarly compromised communications conditions. U.S. Fire Administration/Technical Report Series, "The World Trade Center Bombing: Report and Analysis," (New York , 1993), 14, 32, 38-39, 51, http://www.usfa.dhs.gov/downloads/pdf/publications/tr-076-508.pdf; National Institute of Justice, Office of Justice Programs, U.S. Department of Justice, "Guide to Radio Communications Interoperability Strategies and Products," *Project AGILE Report* (April 2003), 2, http://www.safecomprogram.gov/NR/rdonlyres/8F919F4D-B077-4338-876D-98F440C90606/0/Guide_Radio_Comm_Strategy_and_Products.pdf; see also Donald A. Lund, "The Lessons of Non-Interoperability in Public Safety Communication Systems," *The ATLAS Project, Advanced Technology in Law And Society* (University of New Hampshire, Benchmarks and Blueprints, April 2002), 3-7.

[3] "By some estimates, between $2.5 billion to $5 billion in funds were allocated in fiscal 2004 just for interoperable digital radios built using the Association of Public-Safety Communications Officials' Project 25 standard. The exact amount going solely to interoperability projects can't be determined because much of the funding comes in the form of block grants, by which states receive a large lump sum and allocate the funds as they see fit." Lynnette Luna, "Unclogging the Grant Pipeline**,"** *Mobile Radio Technology*, May 1, 2005.

[4] "Some of the basic weaknesses exposed by September 11 – and, one would have presumed, since fixed – seemed instead to linger. For example, police and other officials were unable to communicate as their cell phones failed and satellite phones took days to arrive." From "Unprepared," *Washington Post,* September 5, 2005, Editorial page.

[5] "Achieving interoperability requires more than technology. Shifting all the elements requires a comprehensive, coordinated strategy. Interoperability is about technological, strategic, tactical, and cultural change, as much as it is an issue of one radio transmitting to another." U.S. Department of Homeland Security, The SAFECOM Program, *SAFECOM: The Road to Interoperability* (Washington, D.C., 2006); also "Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with information assurance." U.S. Department of Defense,

*Instruction Number 4630.8*, June 30, 2004, Section E2.1.32, http://www.dtic.mil/whs/directives/corres/pdf/i46308_063004/i46308p.pdf.

[6] U.S. Department of Homeland Security, *SAFECOM* program information at http://www.safecomprogram.gov/safecom/interoperability/default.htm.

[7] Paul Davidson, "Compatible Radio Systems Would Cost Billions," *USA Today*, December 29, 2005.

[8] *SAFECOM: The Road to Interoperability*.

[9] "As part of the Department of Homeland Security (DHS) Fiscal Year 2005 Homeland Security Grant Program (HSGP) guidance, each Urban Area (UA) receiving Fiscal Year 2005 Urban Area Security Initiative funds must develop a plan to achieve tactical interoperable communications across all jurisdictions in the UA and test the plan through a full-scale exercise." U.S. Dept of Homeland Security, Office of Grants and Training, *Tactical Interoperable Communications, Plan Review Process* (Washington, D.C., 2006).

[10] U.S. Department of Homeland Security, *National Interoperability Baseline Survey* (Washington, D.C.: The SAFECOM Program, 2006), 23.

[11] Ronald P. Timmons, "Radio Interoperability: Addressing the Real Reasons We Don't Communicate Well During Emergencies" (Master's Thesis, Naval Postgraduate School, 2006).

[12] Staff, *The 9/11 Commission Report, Eleventh Public Hearing* (New York: W.W. Norton & Company, 2004).

[13] Further information about *Strong Angel* is available at http://www.strongangel3.net/files/sstr_20061107_web.pdf and http://www.strongangel3.net/files/SAIII_working_report_20061106.pdf.

[14] *SAFECOM: The Road to Interoperability*.

[15] Nita Lewis Miller, Naval Postgraduate School, Monterey, CA, and Lawrence G. Shattuck, U.S. Military Academy, West Point, NY., *A Process Model of Situated Cognition in Military Command and Control,* 2004.

[16] *SAFECOM: The Road to Interoperability*.

[17] Gary Klein, *Sources of Power: How People Make Decisions* (Cambridge, MA: Massachusetts Institute of Technology, 1998), 16.

[18] "A cognitive bias is a tendency to mentally process information in a particular way…people tend to seek out information that confirms their preconceptions and to discount information that disconfirms their preconceptions." Jeffrey P. Richer, Ph.D., Scottsdale (AZ) Community College, Unpublished curriculum, http://www.sc.maricopa.edu/sbscience/psy266/lessons/essays/essay9.html.

[19] Herbert Morrison, *The Hindenburg Broadcast*, May 6, 1937, http://www.eyewitnesstohistory.com/vohind.htm.

[20] "The words stuck in my throat. A sob wanted to replace them. A gulp or two quashed the sob, which metamorphosed into tears forming in the corners of my eyes. I fought back the emotion and regained my professionalism, but it was touch and go there for a few seconds before I could continue." [Sentiments of TV Anchorman Walter Cronkite as he announced the words: "From Dallas, Texas, the flash—apparently official. President Kennedy died at 1 p.m. central standard time—a half hour ago…"], http://www.tvrundown.com/lostfilm.html.

[21] E. A. Butler, et al, "The Social Consequences of Expressive Suppression," *Emotion* 3 (2003): 48–67.

[22] Timmons, "Radio Interoperability."

[23] Butler, "The Social Consequences of Expressive Suppression," 48–67.

[24] Timmons, "Radio Interoperability."

[25] Ibid.

[26]"Jurisdictions will be required to meet the FY 2006 NIMS implementation requirements as a condition of receiving federal preparedness funding assistance in FY 2007." U.S. Department of Homeland Security, *The NIMS Integration Center, National Standard Curriculum Training Development Guidance* (Washington, D.C., 2005).

[27] "The NYPD and the FDNY were two of the preeminent emergency response organizations in the United States. But each considered itself operationally autonomous. Each was accustomed to responding independently to emergencies. By September 11th neither had demonstrated the readiness to respond to an 'Incident Commander' if that commander was an official outside of their Department." National Commission on Terrorist Attacks Upon the United States, Eleventh Public Hearing, May 18, 2004.

[28] National Task Force on Interoperability, "Why Can't We Talk? Working Together To Bridge the Communications Gap to Save Lives. A Guide for Public Officials," February 2003, http://www.safecomprogram.gov/SAFECOM/library/interoperabilitybasics/1159nationaltask.htm.

[29] Robert Zanger, U.S. Department of Justice "Communications Interoperability: It's More About People Than Technology" (presented at the annual international meeting of the Association of Public Safety Communications Officials, Orlando, Florida, August 9, 2006).

[30] Staff, "Police 10-Codes," *Police Chief Magazine*, October 2005. "Homeland Security Secretary Michael Chertoff announced during his remarks at the 112th Annual Conference of International Association of Chiefs of Police in Miami Beach, Florida, on September 27, 2005, that the abolition of the police 10-codes will not be necessary for NIMS compliance." Secretary Chertoff stated, "Under the implementation of the National Incident Management System there has been discussion of requiring the elimination of the 10-code in every day law enforcement communications. However, there was a strong response from the law enforcement community against this proposal, and we listened to your concerns."

[31] Jonathan S. Smith, "Work Channel: A Practical Guide to Improved Radio Communication, A Guide for Public Officials," *9-1-1 Magazine*, July/August 1997.

[32] National Commission on Terrorist Attacks, 2004.